QTONIC QUANTUM

POST QUANTUM READY

ENTERPRISE QUANTUM RISK INTELLIGENCE

HARVEST NOW, DECRYPT LATER: FOOTBALL'S MOST SENSITIVE DATA IS LIVING ON A QUANTUM CLOCK

Cardiac, medical, and identity records from players across 211 nations, collected for life and protected by classical public-key cryptography with a published migration and deprecation horizon. We do not claim to know whether FIFA has a post-quantum plan. This report shows why the risk is material, time-sensitive, and impossible to remediate after the fact.

ISSUED

Public release 11 June 2026 · Classification PUBLIC · Analysis as of April 2026 · Appendix B search re-run on publication date

REPORT TYPE

Public-evidence structural risk analysis. Not a technical audit or internal system inspection.

SCOPE

FIFA global data infrastructure · 211 member associations · 6 confederations

PREPARED BY

Qtonic Quantum Research Team · Miami, FL

FOR THE DECISION-MAKER

00 EXECUTIVE BRIEF

Two minutes. The full analysis follows in Sections 1 through 12.

QTONIC QUANTUM HNDL RISK RATING: CRITICAL C3

Primary driver: zero remediability of cardiac, medical, and identity data, including any biometric elements present, after future decryption. This is a qualitative rating derived from the five-variable HNDL framework in Section 10. It is not a numerical score and is not a prediction of any specific event.

THE PROBLEM

FIFA mandates lifetime-sensitive cardiac, medical, and identity-related data collection across its global competition and registration environment. Where biometric elements are present in identity records, the risk becomes more severe, because those elements cannot be rotated, reissued, or expired. This data is protected by classical public-key cryptography, which has a published migration path under NIST and government guidance even where private-sector timelines vary. The data's confidentiality horizon is measured in decades. The encryption's guarantee is not.

WHY FIFA SPECIFICALLY

- Mandatory, no-opt-out collection across 211 member associations. We have not identified a comparable public case in sport combining mandatory medical screening, global identity registration, 211-member-association concentration, and long-term political sensitivity.
- FIFA Connect concentrates identity and registration data across 211 member associations; medical data moves cross-border through documented workflows.
- A documented pattern of footballers entering national political office, one at head-of-state level. Future political value is unknowable at collection time.
- To our knowledge, and within the sources reviewed (search refreshed June 2026), no major football governing body has publicly announced a PQC migration program.

TIMELINE PRESSURE

The 2026 FIFA World Cup (US / Canada / Mexico, kickoff 11 June 2026) is likely to generate one of the most concentrated bursts of cross-border medical and registration-related data transfers. It begins with no announced PQC migration plan identified in reviewed sources.

RECOMMENDED FIRST STEP

A cryptographic inventory: a complete map of where cardiac, medical, and identity data is stored, how it is encrypted, and which algorithms are in use. This is the prerequisite for any migration program, and it can begin immediately.

THE ASYMMETRY OF REGRET

Migrate and be wrong about the quantum timeline: stronger cryptography deployed, implementation cost incurred, no downside to data subjects. Do not migrate and be wrong: lifetime-sensitive data for players across 211 nations is permanently compromised, with no remediation possible after the fact. The question is whether migration completes before the data's confidentiality window closes.

NAVIGATION

CONTENTS

CORE ANALYSIS

RISK DIMENSIONS & ACTION

APPENDICES

EVIDENCE DISCIPLINE

C1 Documented fact

C2 Reasonable inference

C3 Structural risk analysis

READING NOTE

Every claim in this report is assigned to one of three evidence categories, marked inline where it matters. The integrity of the analysis depends on transparent sourcing and clearly bounded claims.

SECTION ONE

01 EXECUTIVE SUMMARY

This report examines the structural harvest-now-decrypt-later (HNDL) risk facing FIFA's global data infrastructure. It is not an allegation of a specific breach or a specific intelligence operation. It is an analysis of whether the data FIFA collects, the encryption protecting it, and the routes it travels create a risk profile that warrants differentiated attention relative to other organizations facing the same general quantum cryptanalysis threat.

Four characteristics distinguish FIFA's data environment from most other organizations. First, mandatory cardiac and medical data collection with no opt-out, compulsory for all FIFA competitions since 2010. Second, concentration of identity and registration data from 211 member associations through FIFA Connect, with medical and PCMA data moving cross-border through documented workflows rather than a publicly documented central clinical repository. Third, the unpredictable future political significance of the data subjects, with documented cases of professional footballers later entering national political office, including one head-of-state case. Fourth, routine cross-border data transit as a standard operational requirement, across fiber-optic infrastructure publicly documented as subject to bulk signals-intelligence collection.

To our knowledge, no major football governing body has publicly announced a post-quantum cryptography migration program. NIST published the post-quantum standards (FIPS 203, 204, 205) in August 2024. The algorithms exist. Whether or not such a plan exists internally, the risk is material: lifetime-sensitive data, vulnerable public-key cryptography, and no way to remediate after the fact. That is the central finding of this report.

MANDATORY COLLECTION Cardiac and medical data collection compulsory for all FIFA competitions since 2010. No opt-out. Non-adherence is a sanctionable offence.	**211-COUNTRY CONCENTRATION** Identity and registration data from 211 member associations concentrates through FIFA Connect; medical data moves through documented cross-border workflows.
POLITICAL SIGNIFICANCE Documented cases of footballers entering national political office, including one head of state. Future political value is unknowable at collection time.	**NO PUBLIC PQC PLAN** To our knowledge, and within the sources reviewed (refreshed June 2026), no major football governing body has publicly announced a PQC migration program.

Two research preprints published in March 2026 argue that the resource requirements for breaking elliptic-curve cryptography may be substantially lower than previously estimated. Multiple independent programs now describe plausible engineering paths to a cryptographically relevant quantum computer. The precise cost and timeline remain uncertain and are analyzed under three scenarios in Section 6. The thesis of this report does not depend on a specific cost figure or arrival date. It depends on whether such a machine becomes available within the decades-long confidentiality window of cardiac, medical, and identity data. Appendix G demonstrates that the thesis holds under timeline delays extending to 2060 and beyond.

The confidentiality horizon of cardiac ECG data, medical history, genetic predisposition markers, and passport-level identity data is measured in decades, not years. If any portion has been passively collected in transit and stored for future decryption, the exposure cannot be remediated after the fact. The report's recommended actions, beginning with a cryptographic inventory, are set out in Section 10.

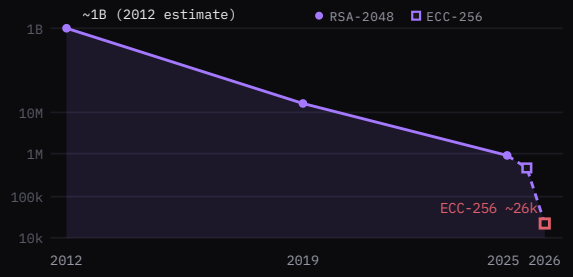
AT A GLANCE

FIG THE RISK IN FOUR VIEWS

Source-based visualizations of the report's core findings. Figures are qualitative and illustrative of the analysis in Sections 6, 9, and 10. They are not predictions and not numerical scores.

FIG.1 RESOURCE ESTIMATES BY PROBLEM CLASS

RSA-2048 factoring and ECC-256 discrete log, shown as separate series. Not directly comparable.



Logarithmic scale, 2012–2026, two problem classes on one scale, not directly comparable across classes. Filled circles, solid line: RSA-2048 (physical qubits). Open squares, dashed segment: ECC-256 (physical-qubit equivalent; the underlying logical-qubit count for ECC-256 is on the order of 1,200–1,450, with the remainder being fault-tolerance overhead). Sources: Gidney / Ekerå 2019; Gidney 2025 (arXiv:2505.15917); Google Research and Cain et al. (arXiv:2603.28627), March 2026 preprints pending peer review. Full table, caveats, and citations: §6.1.

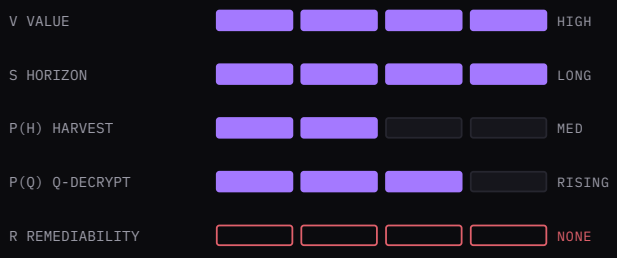
FIG.2 SENSITIVITY VS DECRYPTION WINDOW

Data confidentiality horizon against the plausible arrival of cryptanalysis.

Harvested ciphertext stays exploitable until the data loses sensitivity. Capability plausibly arrives decades inside that window. SRC §6.4, App G.

FIG.3 HNDL RISK PROFILE

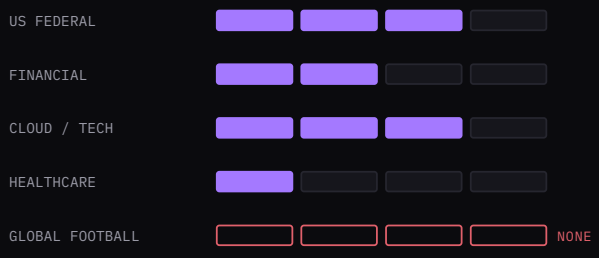
Each variable's contribution to overall risk (qualitative).



Five-variable framework, §10.4. Low remediability (R) is the dominant driver of the CRITICAL rating. Not a numerical score.

FIG.4 PUBLIC PQC MIGRATION POSTURE

Public migration announcements by sector (qualitative).



Reviewed public sources, June 2026. Football: no public plan identified. SRC §9.3, App B.

SECTION TWO

02 EVIDENCE BOUNDARIES & METHODOLOGY

This report distinguishes three categories of evidence throughout. Every claim is assigned to one of these categories, and the category is either stated explicitly or inferable from context. This discipline is intentional.

C1 CATEGORY 1 · DOCUMENTED FACTS

Claims sourced to peer-reviewed literature, official FIFA documentation, government publications, or primary reporting by established news organizations. Examples: FIFA's mandatory PCMA program (British Journal of Sports Medicine; PMC3596861, PMC4413678, PMC12171438); FIFA Connect (inside.fifa.com); Snowden disclosures (The Guardian, The Washington Post); NIST FIPS 203/204/205 (csrc.nist.gov); the public roles of Weah, Romário, and Shevchenko (Britannica, official government records).

C2 CATEGORY 2 · REASONABLE INFERENCES

Claims based on the absence of contrary public evidence or standard industry practice. Examples: that encryption protecting FIFA data in transit uses classical public-key cryptography, and that no major football governing body has publicly announced PQC adoption. See Appendix B for the supporting search methodology.

C3 CATEGORY 3 · STRUCTURAL RISK ANALYSIS

Claims about what could happen given documented infrastructure, known SIGINT capabilities, and the quantum computing trajectory. The HNDL threat model is described by NIST, the Federal Reserve (September 2025), and multiple national cyber authorities. Application of this model to FIFA's specific data environment is the Qtonic Quantum Research Team's analysis. Where a claim falls in Category 2 or 3, bounded language is used: "to our knowledge," "no public evidence can rule out," "may become vulnerable under plausible assumptions."

2.1 LIMITATIONS OF THIS REPORT

- **No access to internal FIFA systems.** We have not inspected FIFA's encryption configuration, network architecture, or internal security policies. All statements about likely encryption posture are inferred from standard industry practice and the absence of public PQC announcements.
- **No access to classified intelligence.** We cannot confirm or deny whether any specific HNDL operation is targeting football data. The threat model is structural, not operational.
- **Search methodology constraints.** The "no public plan" claim is bounded by the methodology in Appendix B. Internal assessments, vendor-initiated upgrades, and unpublished pilots would not be detected.
- **Cost-model uncertainty.** The Shor-machine cost estimates in Section 6 are the Research Team's analysis based on published component pricing and analogous systems. They are not engineering quotes and are illustrative only.
- **Preprint status of key research.** The March 2026 Google Research and Oratomic / Caltech / Berkeley papers are preprints that had not completed peer review as of publication. Resource estimates may be revised upward or downward, and they are theoretical estimates rather than demonstrated hardware.

These limitations are inherent to the subject matter. They do not invalidate the thesis. They define its boundaries.

SECTION THREE

03 FIFA'S DATA COLLECTION INFRASTRUCTURE

FIFA operates one of the largest centralized sports-data infrastructures in the world. It spans 211 member associations across six confederations and serves as the authoritative system for player registration, international transfers, competition management, and medical compliance.

3.1 THE PRE-COMPETITION MEDICAL ASSESSMENT

C1

Following the death of Marc-Vivien Foé during the FIFA Confederations Cup in 2003, FIFA developed a standardized pre-competition medical assessment (PCMA) program. It was first implemented at the 2006 FIFA World Cup in Germany, introduced to women's and youth competitions in 2007 and 2010, and made compulsory for all FIFA competitions by the FIFA Executive Committee. The protocol includes a personal and family medical history questionnaire, a focused physical examination, a 12-lead resting electrocardiogram (ECG), and, when clinically indicated, transthoracic echocardiography, laboratory blood analysis, and exercise stress testing. Non-adherence is a sanctionable offence.

A 2024 global survey of 165 of 211 FIFA member associations found that 81% recommended or mandated cardiac screening. Among those, 92% used a protocol including at least medical history, physical examination, and 12-lead ECG for adult male players.

SRC: Junge et al., BJSM 2012 (PMC3596861) · Dvorak et al., BJSM 2015 (PMC4413678) · FIFA consensus statement, BJSM 2025 (PMC12171438)

3.2 FIFA CONNECT & THE GLOBAL REGISTRATION SYSTEM

C1

FIFA Connect assigns a unique global FIFA ID to every registered player, coach, referee, and official, processing identity documentation across all 211 member associations. Integration was mandated by FIFA Circulars 1654 (Nov 2018) and 1679 (Jul 2019), with a July 2020 deadline. The platform includes the FIFA Connect ID Service, the Data eXchange Platform (DXP), and interfaces with the Transfer Matching System (TMS). When a player transfers internationally, TMS generates an Electronic Player Passport (EPP) compiling registration history from age 12. Medical disclosures are part of the transfer process.

SRC: inside.fifa.com/transfer-system/clearing-house · inside.fifa.com/advancing-football/fifa-connect · support.fifaconnect.org

3.3 DATA TYPES COLLECTED

DATA TYPE	COLLECTION MECHANISM	SENSITIVITY HORIZON
12-lead resting ECG	PCMA (mandatory)	Lifetime
Personal / family medical history	PCMA questionnaire	Lifetime
Echocardiography results	PCMA (when indicated)	Lifetime
Laboratory blood analysis	PCMA (when indicated)	Years → lifetime
Passport / identity data (incl. any biometric elements present)	FIFA Connect registration	Lifetime
Transfer medical disclosures	TMS international transfers	Years → lifetime
Registration history (age 12+)	Electronic Player Passport	Lifetime

CRITICAL CHARACTERISTIC: much of this data, especially cardiac, medical-history, registration-history, and biometric elements where present, cannot be meaningfully rotated, reissued, or expired. A cardiac ECG from 2024 remains valid and sensitive in 2040, 2060, and beyond.

3.4 CROSS-BORDER DATA TRANSIT PATTERNS

Transfer medical disclosures move between clubs in different countries. Tournament PCMA results flow from host-nation facilities to FIFA (Zurich) and confederation offices in Cairo, Kuala Lumpur, Miami, Luque, Auckland, and Nyon. Registration data is exchanged continuously across 211 member associations through FIFA Connect. Each flow crosses at least one national border, many crossing multiple borders through undersea fiber-optic infrastructure.

SECTION FOUR

04 WHY THIS DATA IS DIFFERENT

The HNDL threat applies to every organization using quantum-vulnerable cryptography. This section addresses whether FIFA's specific data environment warrants differentiated attention. The answer is yes. Not because any single factor is unique, but because of the combination.

4.1 MANDATORY COLLECTION, NO OPT-OUT

Players cannot refuse mandatory cardiac and medical assessment for covered competitions, and FIFA Connect processes identity-related records across the global registration environment. Where biometric elements are present, the irreversibility risk becomes more severe. The PCMA has been compulsory for all FIFA competitions since 2010, with non-adherence a sanctionable offence. Few health systems present the same combination of mandatory collection, global federation, athlete identity, and cross-border governance, and we are not aware of one that mandates cardiac screening across 211 countries with no right of refusal.

4.2 UNMATCHED CONCENTRATION ACROSS JURISDICTIONS

FIFA Connect concentrates identity and registration data, including any biometric elements present, on players from virtually every nation. Medical and PCMA data move cross-border through documented workflows over the same monitored routes; public sources do not establish a single central clinical repository. The centralized design of FIFA Connect means interception at key transit hubs, particularly those serving FIFA headquarters in Zurich or major confederation offices, could expose identity and registration data from a disproportionately large number of member associations at once. That concentration ratio is difficult to match outside national passport systems.

4.3 UNPREDICTABLE FUTURE POLITICAL VALUE

Footballers are collected as athletes. Some later become presidents, senators, and wartime political leaders (see Section 7). FIFA is one of the only organizations that compels lifetime-sensitive data collection from a large population whose future political significance is unknowable at the time of collection.

4.4 ROUTINE CROSS-BORDER TRANSIT

FIFA's data crosses borders as standard operations, not as the exception. Those transit routes cross fiber-optic infrastructure publicly documented as subject to bulk signals-intelligence collection. The attack surface is the entire set of international data routes the sport requires to function, with no path to avoid it without ceasing operations.

4.5 COMPARISON TO OTHER SECTORS

FACTOR	HOSPITAL	LAW FIRM	DEFENSE CONTRACTOR	FIFA
Collection voluntary?	Yes	Yes	Varies	**No (sanctionable)**
Jurisdictional scope	1 country	1–3	1–5	**211 countries**
Subjects become political?	Rarely	Sometimes	Sometimes	**Documented pattern**
Routine cross-border transit?	Rarely	Sometimes	Yes (classified)	**Yes (standard ops)**
Data rotatable?	No	No	No	**No**

4.6 COMPARABLE ORGANIZATIONS

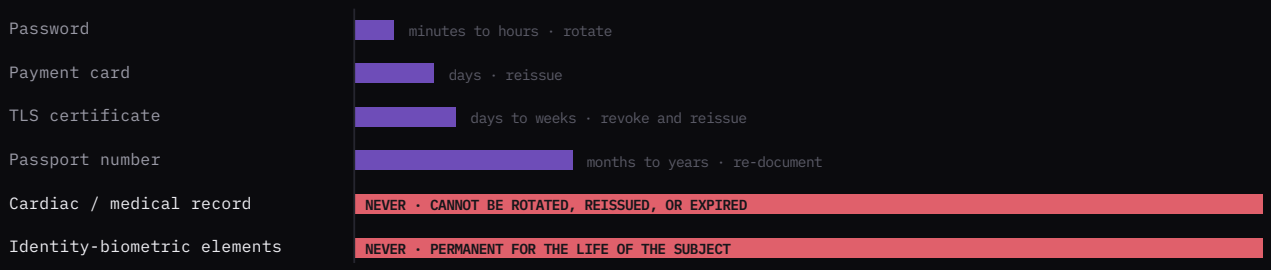
International Olympic Committee. The IOC requires medical examinations but operates on a quadrennial cycle with roughly 10,500 athletes per event. It does not maintain a year-round centralized registration system comparable to FIFA Connect across 211 federations. The episodic nature of collection substantially reduces the attack surface relative to FIFA's continuous flows.

World Anti-Doping Agency. WADA's ADAMS system tracks athlete whereabouts and biological-passport data globally and is the closest analogue in reach. But its data is primarily biochemical rather than cardiac or identity-biometric, and sensitivity horizons are typically career-length, not lifetime.

National passport systems. The closest analogue in biometric sensitivity and mandatory participation. But they are operated by a single sovereign with dedicated security infrastructure and legal frameworks. FIFA operates a comparable footprint without sovereign-grade security, across 211 jurisdictions of widely varying cybersecurity maturity. The least-protected member association sets the ceiling for the whole network.

FIG.5 TIME TO REMEDIATE AFTER COMPROMISE

How quickly a compromised credential or record can be replaced. Conceptual scale, qualitative.



Remediability is the dominant variable in the HNDL framework (Fig.3). A compromised password is rotated and a compromised card is reissued. A decrypted cardiac record, and any biometric elements present in an identity record, cannot be remediated by any future action. Qualitative comparison. C3

SECTION FIVE

05 THE HARVEST-NOW-DECRYPT-LATER THREAT MODEL

HNDL requires three conditions to be simultaneously true. First, the ability to passively collect encrypted traffic in transit. Second, the ability to store that traffic indefinitely at low cost. Third, a reasonable expectation that the encryption will become breakable within the useful lifetime of the data. For lifetime-sensitive data, even a distant quantum timeline creates present-day exposure. The harvest happens now. The decryption happens later. The victim never knows.

01 · PASSIVE COLLECTION	02 · INDEFINITE STORAGE	03 · FUTURE DECRYPTION
A fiber tap captures encrypted traffic silently, without altering the signal.	Cold storage at roughly $0.01–0.02 per GB per month. The marginal cost of retention is negligible.	A cryptographically relevant quantum computer running Shor's algorithm breaks the recorded key exchange.

5.1 HOW EASY IS THE HARVEST

C1

As much as 99% of intercontinental internet traffic travels through undersea fiber-optic cables. At landing points and amplification stations (roughly every 80 km for undersea cables), data can be copied without interrupting flow. Documents disclosed by Edward Snowden in 2013 revealed GCHQ's Tempora program collected approximately 21 million gigabytes per day from fiber-optic cables. INCENSER pulled approximately 14 billion pieces of internet data per month from a single submarine cable. Equipment for fiber-optic interception is commercially available at relatively low cost.

WHAT THE HARVEST REQUIRES / COSTS / WHY IT IS UNDETECTABLE

Requires: access to fiber infrastructure at a landing point, amplification station, or cooperating telco. No breach of FIFA systems, no malware, no insider. **Costs:** for a nation-state with existing SIGINT infrastructure, effectively nothing beyond marginal cold storage. **Undetectable:** passive tapping does not alter the signal. No alarm fires. No log entry is created. The target has no forensic visibility.

5.2 DOCUMENTED BULK COLLECTION PROGRAMS

C1

PROGRAM	OPERATOR	METHOD	SCALE
Tempora	GCHQ (UK)	Fiber tapping via cooperating telcos	~21M GB/day
INCENSER	NSA / GCHQ	Single submarine cable (Asia–Europe)	~14B pieces/mo
Upstream	NSA (US)	Fiber infrastructure on US soil	Classified
USS Jimmy Carter	US Navy / NSA	Physical submarine cable tapping	Classified

SRC: The Guardian (Tempora, Jun 2013) · Channel 4 News / Süddeutsche Zeitung (INCENSER, Nov 2014) · Privacy International · AP (USS Jimmy Carter, 2005) · Wilson Center (Optical Core Infrastructure, Feb 2024)

5.3 TECHNICAL ANALYSIS: ENCRYPTION IN TRANSIT

C2

FIFA has not publicly disclosed its encryption configuration. Based on standard industry practice, web-based data exchanges are likely protected by TLS 1.2 or 1.3 with classical key exchange (ECDHE-RSA or X25519). Both are quantum-vulnerable. TLS 1.3 provides forward secrecy against classical key compromise but does not protect against quantum cryptanalysis of a recorded session. HNDL captures the entire session including the ephemeral key exchange, which becomes breakable under Shor's algorithm. Hybrid post-quantum key agreement is already deployed or tested in major production environments, including Chrome and Cloudflare. Signal has separately deployed post-quantum protections in its messaging protocol. The technology to protect data flows of this kind exists today. To our knowledge, and within the sources reviewed, no football governing body has publicly announced deploying it.

5.4 HISTORICAL PRECEDENTS

East German Stasi files. Medical and personal data collected over four decades was weaponized for coercion after reunification. Data collected under one arrangement can be weaponized under a different one. **OPM breach (2015).** Security-clearance files of 21.5 million people, including decades-old medical information, were exposed. Centralized identity data retains intelligence value indefinitely. **Equifax breach (2017).** PII of 147 million individuals exposed. Unlike passwords, SSNs and biometrics cannot be rotated. The exposure is permanent.

SECTION SIX

06 THE QUANTUM CRYPTANALYSIS TIMELINE

ROLE IN THESIS: the central argument does not depend on a specific quantum timeline or machine cost. It depends on whether a cryptographically relevant quantum computer becomes available within the decades-long sensitivity horizon of the data FIFA collects. Cost estimates below are illustrative, not load-bearing.

6.1 RESOURCE ESTIMATES BY PROBLEM CLASS

YEAR	TARGET	PHYSICAL QUBITS	SOURCE
2012	RSA-2048	~1 billion	Van Meter et al.
2019	RSA-2048	~20 million	Gidney / Ekerå (Google), peer-reviewed
2025	RSA-2048	~1 million	Gidney (Google, updated)
31 Mar 2026	ECC-256	<500,000	Google Research team PREPRINT
30 Mar 2026	ECC-256	~26,000	Cain et al. (Oratomic / Caltech / Berkeley) PREPRINT

The two March 2026 preprints report physical-qubit figures that appear to conflict: the Google Research team estimates fewer than 500,000 physical qubits for ECC-256, while Cain et al. estimate roughly 26,000 for the same elliptic-curve problem (their headline figure, as few as 10,000 reconfigurable atomic qubits, applies to factoring). The gap is not an error in either paper. It reflects different error-correction assumptions: conservative overhead ratios in the Google work, high-performing qLDPC codes on reconfigurable neutral-atom hardware in Cain et al. Both agree on the direction: requirements are substantially lower than prior estimates. This report treats both as lower-bound illustrations of a compressing requirement, not engineering specifications. The structural thesis rests on the peer-reviewed 2019 baseline and the data's sensitivity horizon (Appendix G), not on either preprint.

PHYSICAL VS LOGICAL: the counts above are physical qubits. For ECC-256 the logical-qubit requirement is on the order of 1,200–1,450; the remainder is fault-tolerance overhead. Scott Aaronson, a noted skeptic of quantum-computing hype, called the Cain et al. result the more substantive of the two papers while cautioning that neither demonstrates a new experimental capability. This report adopts that caution: these are theoretical estimates, not demonstrated hardware.

6.2 ILLUSTRATIVE COST SCENARIOS C3

OPTIMISTIC	BASE CASE	PESSIMISTIC
~$10–20M	**~$15–30M**	**~$30–60M+**
2029–2030	2030–2032	2033–2036+
qLDPC near theoretical ratios, 99.9%+ gate fidelity. Fastest convergence of engineering gaps.	Moderate overhead ratios, 99.8–99.9% fidelity. Standard engineering progression.	qLDPC underperforms at 3–5× overhead. Fidelity stalls. Classical control lags.

ORDER-OF-MAGNITUDE ONLY. Derived from preprint inputs not yet peer-reviewed. Not engineering quotes. The thesis holds whether the machine costs $20M or $200M, provided it arrives within the data's sensitivity horizon.

6.3 ENGINEERING GAPS & FALSIFIABILITY

- **Gate fidelity.** Current best ~99.7%; target 99.9%+. Failure pushes cost toward $40–60M+.
- **qLDPC at scale.** 10:1 ratio is theoretical. At 30:1 the machine needs ~78,000 qubits (~3× cost).
- **Classical control.** Tens of thousands of qubits, microsecond precision, ~10 days continuous operation. An unprecedented engineering challenge.

This thesis would be significantly weakened if any of the following were demonstrated. First, a publicly announced and documented PQC migration program at FIFA or a major confederation, already underway with verifiable deployment evidence. Second, FIFA transit architecture using end-to-end post-quantum encryption or avoiding monitored fiber entirely. Third, PCMA data remaining entirely within host-country systems, never transmitted cross-border. Fourth, a quantum cryptanalysis timeline extending beyond 2045, shrinking the overlap with the data's sensitivity horizon to a negligible range. Each condition is specific, verifiable, and testable. We are not aware of evidence supporting any of them as of April 2026.

6.4 TIMELINE RESILIENCE

The critical question is not when a quantum computer will be built. It is whether one will be built within the sensitivity horizon of the data. A player screened at age 22 in 2024 will be 58 in 2060.

QUANTUM TIMELINE	PLAYER AGE AT DECRYPTION	DATA STILL SENSITIVE?	THESIS HOLDS?
2030 · optimistic	28	Yes (cardiac, medical, identity)	Yes
2035 · base case	33	Yes	Yes
2040 · pessimistic	38	Yes	Yes
2045 · very pessimistic	43	Yes	Yes
2050 · extreme delay	48	Yes	Yes
2060 · far horizon	58	Yes (cardiac, genetic, identity)	Yes

Full resilience analysis in Appendix G. Under every scenario examined, including a 36-year delay, the data remains sensitive at the time of potential decryption.

6.5 INDEPENDENT EXPERT CONSENSUS C1

The report's thesis does not rest on the company's own view of the timeline. The Global Risk Institute, with evolutionQ, has surveyed quantum-computing experts annually since 2019. Its seventh edition (dated 9 March 2026, authored by Michele Mosca and Marco Piani, 26 respondents) reports that a cryptographically relevant quantum computer is considered quite possible within ten years and likely within fifteen, the highest ten-year estimate in the survey's history. At the twenty-year mark, a large majority of respondents place the probability at fifty percent or higher. That survey frames the decision through the Mosca Inequality: if the sensitivity life of the data plus the migration time exceeds the time to a quantum threat, the data is already at risk. For cardiac, genetic, and identity records with lifetime sensitivity, that inequality is satisfied under essentially every published estimate.

SECTION SEVEN

07 THE POLITICAL EXPOSURE DIMENSION

Intelligence services have operational incentives to collect broadly and sort later. No analyst in 2006 could predict which players being screened at a FIFA World Cup would hold national office by 2018. The documented pattern of footballers entering political life, including at head-of-state level, establishes that FIFA's data subjects carry an unpredictable future political significance that compounds the HNDL risk in ways that are unusual relative to most hospital or corporate data environments.

7.1 FOOTBALLERS WHO ENTERED NATIONAL POLITICAL OFFICE

C1

George Weah · Liberia. Professional career 1985–2003 at top European clubs. FIFA World Player of the Year 1995. Elected 25th President of Liberia in 2017. Served 2018–2024.

Romário · Brazil. Professional career 1985–2007. 1994 World Cup Golden Ball. Elected to the Brazilian Chamber of Deputies in 2010. Elevated to the Federal Senate in 2014, where he currently serves.

SRC: Britannica · official Liberian government biography (emansion.gov.lr) · FIFA.com official profiles · Brazilian Federal Senate public records

7.2 ATHLETES WHO ENTERED POLITICS, PUBLIC OFFICE, OR NATIONAL SPORTS GOVERNANCE

NAME	SPORT	COUNTRY	POLITICAL ROLE
George Weah	Football	Liberia	President (2018–2024)
Romário	Football	Brazil	Federal Senator (2014–)
Andriy Shevchenko	Football	Ukraine	President, Ukrainian FA (2024)
Imran Khan	Cricket	Pakistan	Prime Minister (2018–2022)
Manny Pacquiao	Boxing	Philippines	Senator (2016–2022)
Vitali Klitschko	Boxing	Ukraine	Mayor of Kyiv (2014–)
Hakan Şükür	Football	Turkey	Member of Parliament (2011–2015)
Pelé	Football	Brazil	Minister of Sport (1995–1998)

7.3 THE COERCION RISK MODEL

C3

The coercion risk is structural, not an allegation about any named individual. Data treated as routine health information at collection can become leverage against someone later operating in public life. No intelligence service can predict which current player will matter politically in 2045.

FIG.6 THE COLLECTION-TO-OFFICE GAP

Documented pattern shown generically: in the 7.1 case, election to head of state came 14 years after retirement. Harvested ciphertext from year 0 remains exploitable throughout. No statement is made about any individual's data. C3

SECTION EIGHT

08 IDENTITY FRAUD BEYOND SPORT

C3 STRUCTURAL RISK ANALYSIS

The claims in this section are structural inferences about what decrypted data could enable, not documented incidents. No specific incident of this nature has been documented.

FIFA Connect processes passport-level identity documentation across 211 member associations. Depending on the specific biometric data elements present in a registration record, a decrypted passport-level identity record from FIFA Connect, including any biometric elements present in that record, would, structurally, present exploitation vectors similar to identity documents obtained from government databases.

DOCUMENT FORGERY C3

Biometric elements from FIFA Connect records would structurally enable fraudulent identity documents across 211 jurisdictions of varying security control.

IMPERSONATION C3

Passport-level identity data in decrypted form would structurally enable impersonation or synthetic-identity creation at a scale comparable to national identity databases.

PERMANENT EXPOSURE

Unlike a password or access credential, a compromised biometric cannot be reissued, rotated, or expired. The exposure is permanent and irremediable.

A state or non-state actor with access to decrypted FIFA Connect records would, structurally, possess a database of passport-grade identity records spanning 211 nations: a resource with intelligence, criminal, and geopolitical applications well beyond the domain of sport. The permanence of biometric data makes this the highest-irreversibility risk in the entire threat model. This section analyzes the structural properties of the data, not alleged events.

SECTION NINE

09 THE ENCRYPTION POSTURE OF GLOBAL FOOTBALL

9.1 ABSENCE OF PUBLIC PQC ANNOUNCEMENTS

C2

To our knowledge, as of 11 June 2026 and within the search scope described in Appendix B (refreshed on the publication date), no major football governing body has publicly announced a post-quantum cryptography migration program. This includes FIFA, all six confederations (AFC, CAF, CONCACAF, CONMEBOL, OFC, UEFA), and major domestic leagues. The absence is consistent across all tiers of the global football governance structure.

9.2 NIST DEPRECATION TIMELINE

C1

- **Aug 2024** · NIST publishes FIPS 203/204/205 (ML-KEM, ML-DSA, SLH-DSA).
- **Jan 2027** · CNSA 2.0 requires PQC-compliant acquisitions for new national security systems.
- **2029** · Google's internal PQC migration deadline. Signals enterprise-grade feasibility within this window.
- **2030** · NIST IR 8547 (initial public draft) targets deprecation of RSA/ECDSA across US federal infrastructure.
- **2035** · NIST full disallowance of RSA/ECDSA in new implementations, per the same draft.

9.3 MIGRATION PROGRESS BY SECTOR

SECTOR	PQC STATUS (PUBLIC)
US Federal Government	Mandated. Inventory phase underway. CNSA 2.0 deadlines from 2027.
Financial Services	Active pilots. SWIFT and major banks formally assessing migration.
Cloud / Big Tech	Google (2029 internal deadline), Apple (iMessage PQ3), Signal (PQXDH deployed).
Healthcare	Early awareness. Limited public announcements.
Global Football	**No public announcements to our knowledge. No migration timeline. No public inventory commitment.**

9.4 MIGRATION COMPLEXITY FOR FEDERATED GOVERNANCE

- **Heterogeneous IT.** 211 member associations of vastly different cybersecurity maturity. A compromise at any single node creates exposure across the whole network. The system is only as protected as its least-protected member.
- **Vendor dependency.** Many associations use third-party systems. FIFA cannot directly control their encryption stack or mandate upgrades unilaterally.
- **Certificate management at scale.** Migrating TLS certs, API keys, and VPN configurations across 211 nations requires extensive multi-jurisdictional coordination.

Timeline estimate. 3–5 years from committed decision to full deployment across all member associations. If started in 2026, completion lands 2029–2031, aligned with the NIST draft deprecation window. Deferred to 2028, completion lands 2031–2033, overlapping the quantum timeline under base and optimistic scenarios. Every year of delay narrows the safe migration window.

9.5 DATA PROTECTION & REGULATORY EXPOSURE

GDPR. EU player data is subject to Article 32 (appropriate technical measures), Article 9 (special categories including health data), and Article 25 (data protection by design). Known cryptographic deprecation may trigger a duty to assess quantum risk. **Swiss nFADP (2023).** Requires appropriate technical measures for sensitive personal data; FIFA is directly subject. **Player data rights.** Rights to information (Art. 13/14), access (Art. 15), and erasure (Art. 17). The compulsory, no-opt-out nature of the PCMA substantially increases regulatory sensitivity.

SECTION TEN

10 WHAT FIFA WOULD NEED TO DO

A post-quantum migration is a multi-year engineering and governance initiative, not a software patch. For an organization with FIFA's jurisdictional complexity, it requires sustained executive commitment, dedicated resources, and a structured framework. The technology exists today. What is required is the decision to begin.

01 **CRYPTOGRAPHIC INVENTORY**

Map where cardiac, medical, and identity data is stored, how it is encrypted at rest and in transit, which algorithms are in use (RSA, ECDH, ECDSA, TLS versions), and which systems are migration-agile. This Cryptographic Bill of Materials (CBOM) is the prerequisite for everything that follows. Without it, migration cannot be scoped or sequenced.

02 **NETWORK VISIBILITY**

Cryptographic posture cannot be assessed at headquarters alone. Visibility into the posture of 211 member associations, six confederations, and major club systems is essential, because a compromise at any node can expose linked records or flows, depending on segmentation and access controls. The US federal CBOM program offers a working template for large distributed organizations.

03 **MIGRATION TIMELINE**

NIST standards are finalized. Enterprise PQC migration requires 2–5 years. Begun in 2026, completion aligns with the draft 2030 NIST deprecation target. Deferred to 2028+, the window narrows and may overlap the quantum timeline under optimistic and base-case scenarios. The 2026 FIFA World Cup is a near-term forcing function for concentration of cross-border medical data.

04 **RISK QUANTIFICATION FRAMEWORK**

HNDL risk is a function of five variables: V (value of decrypted data), S (sensitivity horizon), P(H) (probability of harvest), P(Q) (probability of quantum decryption within S), and R (remediability). FIFA's cardiac, medical, and identity data scores high V, long S, non-trivial P(H), increasing P(Q), and zero R. These data types warrant highest prioritization within any migration sequencing.

05 **CYBER INSURANCE & FINANCIAL RISK TRANSFER** C3

Cyber insurers are tightening underwriting around systemic and catastrophic risk. The market has already moved to exclude state-backed and war-related cyber losses, and reinsurers are actively reframing how large, correlated cyber events are defined and priced. Harvest-now-decrypt-later sits squarely in that systemic-risk category: a single cryptanalytic advance could expose many insureds at once. It is reasonable to expect quantum readiness to enter underwriting questionnaires and pricing as that category matures. For a CFO, this is a plausible near-term financial trigger that does not depend on the quantum timeline being resolved, only on insurers treating quantum exposure as material.

SECTION ELEVEN

11 THE HONEST COUNTER

THE STRONGEST OBJECTION

Everything in this report is also true, in general terms, for hospitals, banks, law firms, and defense contractors. FIFA is not uniquely vulnerable. It is one node in a global system failing to prepare for quantum cryptanalysis. Given finite resources, should FIFA prioritize ahead of healthcare or national defense? That is a legitimate resource-allocation question.

WHY THE COUNTER DOES NOT HOLD

The proportionality objection concedes the risk exists and disputes only the priority ranking. This report demonstrates the risk is material. The combination of four characteristics, mandatory no-opt-out collection, 211-country concentration, a documented pattern of subjects entering political life, including at head-of-state level, and routine cross-border transit across documented SIGINT infrastructure, distinguishes FIFA from any single-sector comparator. No single factor is unique. The combination is.

COST OF ACTING AND BEING WRONG

The organization deploys stronger cryptography than it turns out to need. Implementation cost is incurred. There is no downside to data subjects. Cryptographic posture improves regardless of the quantum timeline.

COST OF NOT ACTING AND BEING WRONG

Lifetime-sensitive medical and identity data for players across 211 nations becomes permanently compromised, with no remediation possible. Cardiac ECGs, genetic markers, and biometric elements, where present, cannot be reissued. Political coercion risk materializes for former players in public life. Regulatory exposure under GDPR and nFADP activates.

> **THE ASYMMETRY OF REGRET**
>
> The cost of migrating and being wrong is manageable. The cost of not migrating and being wrong is catastrophic and permanent. That asymmetry does not depend on a specific quantum timeline. It depends only on the data being sensitive for longer than the encryption is guaranteed to hold.

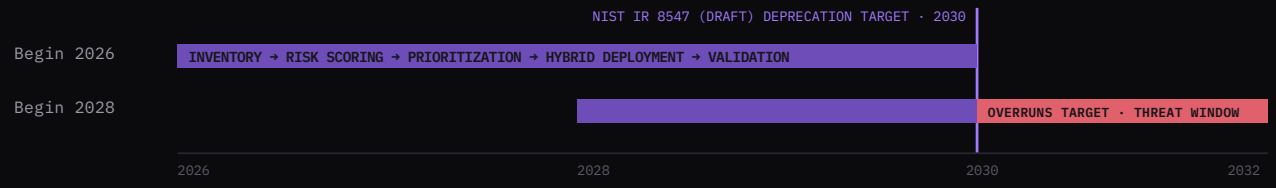
SECTION TWELVE

12 CONCLUSIONS

01	FIFA mandates collection of lifetime-sensitive cardiac, medical, and identity-related data from players across 211 nations through documented programs.	C1
02	That data crosses borders routinely through fiber-optic infrastructure documented as subject to bulk SIGINT collection.	C1 C2
03	To our knowledge, no major football governing body has publicly announced PQC migration. None identified in the sources reviewed (search refreshed June 2026).	C2
04	The highest-risk elements cannot be meaningfully rotated or expired. The sensitivity horizon is measured in decades.	C3
05	Resource requirements for quantum cryptanalysis are compressing across multiple independent programs. The thesis does not depend on any specific estimate, only on whether the machine arrives within the data's sensitivity horizon.	C1 C3
06	Professional footballers have entered national political office, including one documented head-of-state case.	C1

One of the most sensitive data environments in professional sports is protected by cryptography with a published deprecation timeline. The data behind it lasts a lifetime. To our knowledge, and within the sources reviewed, no public plan for what comes next has been identified in football.

FIG.7 MIGRATION RUNWAY VS DEPRECATION HORIZON



Enterprise PQC migration historically requires 2–5 years (Section 10). Begun in 2026, a five-phase program completes near the draft 2030 federal deprecation target. Deferred to 2028, the same program overruns the target and overlaps the optimistic-to-base-case cryptanalysis scenarios in Section 6.2. Illustrative timeline. C3

RECOMMENDED NEXT STEP

The recommended first action is a cryptographic inventory: a complete map of where cardiac, medical, and identity data is stored, how it is encrypted, and which algorithms are in use. It is not a speculative exercise. It is the prerequisite for any migration program and can begin immediately. The Qtonic Quantum Research Team is available to brief FIFA security leadership, designated counsel, or other qualified institutional stakeholders on cryptographic-inventory methodology for federated, cross-border data environments.

APPENDIX A

SOURCE DOCUMENTATION & EVIDENCE INDEX

[1] Junge et al. "Feasibility of precompetition medical assessment at FIFA World Cups." BJSM 2012. PMC3596861.
[2] Dvorak et al. "F-MARC: promoting prevention of sudden cardiac arrest in football." BJSM 2015. PMC4413678.
[3] Baggish, Papadakis et al. "Recommendations for cardiac screening and emergency action planning in youth football: a FIFA consensus statement." BJSM 2025. PMC12171438.
[4] FIFA global cardiac screening survey, conducted Feb–Jul 2024, 165/211 MAs responding (78%); 81% of respondents recommend or mandate screening. Published BJSM 2025 (doi:10.1136/bjsports-2025-109751).
[5] FIFA. inside.fifa.com/advancing-football/fifa-connect/programme-details.
[6] FIFA. inside.fifa.com/transfer-system/clearing-house/systems-integration.
[7] FIFA. support.fifaconnect.org (FIFA Connect ID overview, registration guides).
[8] FIFA Circulars 1654 (Nov 2018) and 1679 (Jul 2019). Integration deadline Jul 2020.
[9] Snowden / Tempora: The Guardian, 21 Jun 2013. "GCHQ taps fibre-optic cables."
[10] INCENSER: Channel 4 News / Süddeutsche Zeitung (Nov 2014), reported within the broader WINDSTOP collection (The Washington Post, 2013); Privacy International (2013).
[11] USS Jimmy Carter: Associated Press, February 2005.
[12] Wilson Center. "Optical Core Infrastructure." February 2024.
[13] Privacy International. "GCHQ Tapping International Fibre-Optic Cables." 2013.
[14] Google Research team. ECC-256 resource estimate (<500,000 physical qubits). 31 Mar 2026. [Preprint, not peer-reviewed]
[15] Cain et al. "Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits." arXiv:2603.28627. 30 Mar 2026. [Preprint, not peer-reviewed]
[16] NIST. FIPS 203 (ML-KEM), 204 (ML-DSA), 205 (SLH-DSA). August 2024. csrc.nist.gov.
[17] NIST IR 8547, initial public draft (Nov 2024). Transition to Post-Quantum Cryptography Standards. Draft targets: deprecation 2030, disallowance 2035.
[18] George Weah: Britannica; official Liberian government biography (emansion.gov.lr); Al Jazeera; France24.
[19] Romário: FIFA.com official player profile; Brazilian Federal Senate public records.
[20] Shevchenko: UEFA.com official profile; Ukrainian Association of Football announcement, 2024.
[21] Qtonic Quantum cost analysis. Internal. Based on published component pricing. March 2026.
[22] Federal Reserve. Harvest-now-decrypt-later risk paper. September 2025.
[23] Mosca & Piani. "Quantum Threat Timeline Report 2025." Global Risk Institute / evolutionQ, 9 Mar 2026 (seventh edition, 26 expert respondents).

APPENDIX B

B METHODOLOGY: 'NO PUBLIC PLAN' CLAIMS

The claim that no major football governing body has publicly announced PQC migration is based on the following bounded search methodology, disclosed in full to support informed interpretation of the claim's scope.

SEARCH SCOPE

FIFA, all six confederations (AFC, CAF, CONCACAF, CONMEBOL, OFC, UEFA), the top five domestic leagues by revenue (Premier League, La Liga, Bundesliga, Serie A, Ligue 1), and the top 20 clubs by revenue (Deloitte Football Money League 2025).

SEARCH METHOD

Web searches conducted between 15 March and 5 April 2026 using Google, Bing, and direct searches of organizational websites. Terms included combinations of [organization name] + "post-quantum," "PQC," "quantum-safe," "quantum-resistant," "FIPS 203," "ML-KEM," "cryptographic migration."

RESULT

Zero public announcements of PQC migration programs were identified across any entity in scope. The search was refreshed on the publication date, 11 June 2026, and no contrary public announcement was identified. This supports the claim as stated, "to our knowledge, no major football governing body has publicly announced," but does not prove no internal activity exists.

EXCLUSIONS & LIMITATIONS

We did not search private or internal communications, non-public board minutes, vendor contracts, or classified government assessments. This methodology would not detect unpublished internal assessments, vendor-initiated upgrades that are not publicly announced, or migration activity within IT infrastructure providers serving football organizations. The claim is bounded accordingly: it establishes the public posture, not the internal reality.

> **OPERATIONAL NOTE FOR DELIVERY**
>
> Because this is a public release, the central claim is the one most exposed to falsification by a subsequent public announcement. The scoped search was refreshed on the publication date. It should be re-run and timestamped again immediately before any further reissue or update.

APPENDIX C

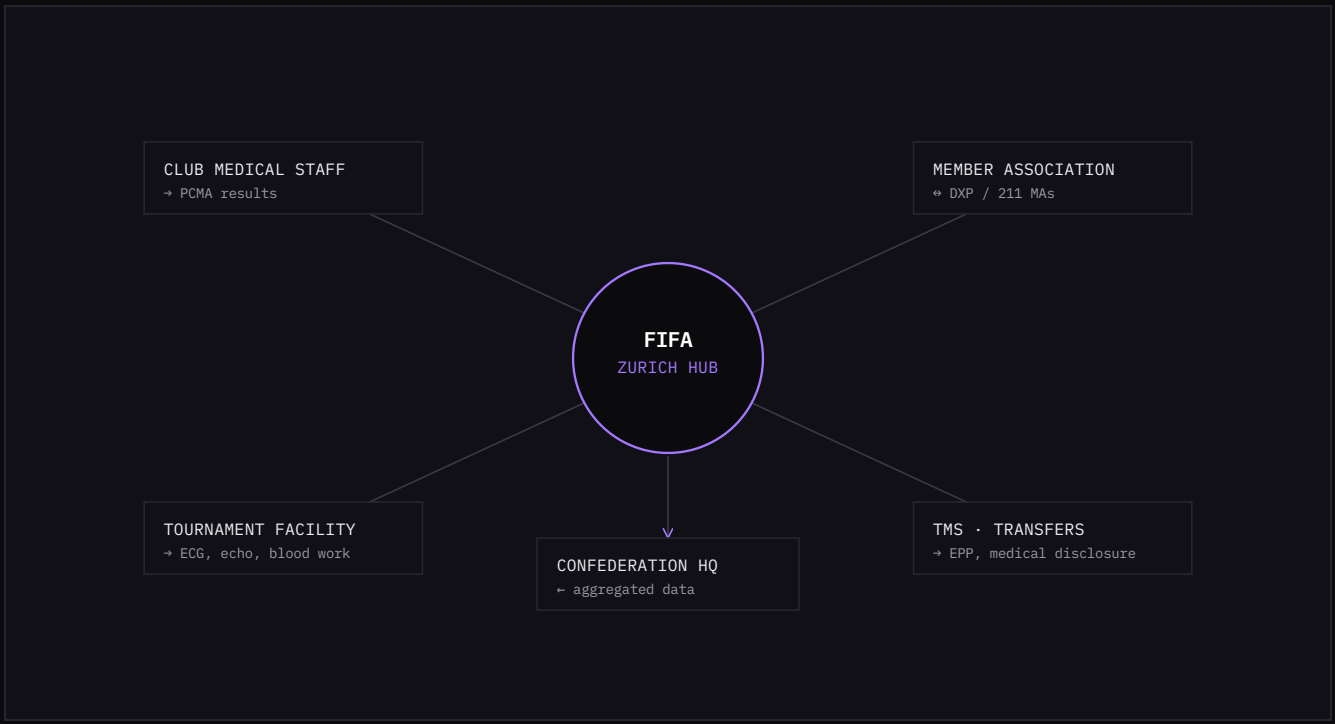
C GLOSSARY

CBOM	Cryptographic Bill of Materials. Inventory of all cryptographic assets in an organization.
CNSA 2.0	NSA's updated algorithm guidance for National Security Systems.
ECC / ECDSA / ECDH	Elliptic Curve Cryptography and its signature/key-exchange variants. Vulnerable to Shor's algorithm.
ECG	Electrocardiogram. Recording of the heart's electrical activity. Collected under the mandatory PCMA.
EPP	Electronic Player Passport. FIFA document compiling registration history from age 12.
FIPS 203/204/205	NIST post-quantum standards: ML-KEM, ML-DSA, SLH-DSA.
HNDL	Harvest Now, Decrypt Later. Threat model for future quantum decryption of today's encrypted data.
ML-KEM	Module-Lattice Key Encapsulation Mechanism. NIST FIPS 203.
ML-DSA	Module-Lattice Digital Signature Algorithm. NIST FIPS 204.
NSM-10	White House directive requiring federal cryptographic inventory and PQC migration.
PCMA	Pre-Competition Medical Assessment. FIFA's mandatory medical screening protocol.
PQC	Post-Quantum Cryptography. Algorithms designed to resist attacks by quantum computers.
qLDPC	Quantum Low-Density Parity-Check codes. Error-correction codes with lower overhead requirements.
RSA	Rivest-Shamir-Adleman. Public-key cryptosystem vulnerable to Shor's algorithm.
Shor's Algorithm	Quantum algorithm (1994) capable of breaking RSA and ECC encryption at scale.
TMS	Transfer Matching System. FIFA's international player-transfer processing system.

APPENDIX D

D FIFA DATA FLOW DIAGRAM

Conceptual. Each edge represents a cross-border data-transit event. The FIFA Connect hub processes identity and registration data continuously across all 211 member associations, the primary HNDL attack surface.



FROM	TO	DATA TYPE	TRIGGER
Club Medical Staff	Member Association	PCMA results	Registration
Member Association	FIFA (Zurich)	PCMA compliance, registration	Competition deadline
FIFA (Zurich)	Confederation HQ	Aggregated data	Tournament admin
Releasing Club	TMS (FIFA)	Transfer medical, history	Intl transfer
TMS (FIFA)	Acquiring Club	EPP, medical disclosure	Transfer completion
FIFA Connect	211 MAs	FIFA ID, status updates	Continuous

APPENDIX E

2026 WORLD CUP HOST-COUNTRY DATA PROTECTION

The 2026 FIFA World Cup (US / Canada / Mexico, kickoff 11 June 2026) is likely to generate one of the most concentrated bursts of cross-border medical and registration-related data transfers. Tournament PCMA data for players representing 211 nations will transit between host-country facilities, FIFA headquarters in Zurich, and all six confederation offices, within a compressed timeframe, across three distinct legal jurisdictions.

JURISDICTION	PRIMARY LAW	HEALTH-DATA CLASSIFICATION	CROSS-BORDER RULES
United States	HIPAA, state laws	Health data. Potentially PHI depending on covered-entity / business-associate context. State privacy & biometric laws (e.g., BIPA, CCPA) may also apply	Sectoral
Canada	PIPEDA	Sensitive personal info	Adequacy-based
Mexico	LFPDPPP	Sensitive (health, biometric)	Consent-based
EU (origin)	GDPR	Special category (Art. 9)	SCCs / BCRs
Switzerland (HQ)	nFADP (2023)	Sensitive personal data	Adequacy list

THE 2026 INFLECTION POINT

If PQC is implemented before the tournament, it protects one of the most concentrated bursts of cross-border medical and registration-related data in FIFA's annual calendar. If not, that data joins existing potentially harvestable traffic, and cannot be recalled, rotated, or expired after the fact.

APPENDIX F

TIMELINE OF KEY EVENTS

DATE	EVENT
1994	Shor's algorithm published. Theoretical basis for quantum cryptanalysis of RSA and ECC.
2003	Death of Marc-Vivien Foé during FIFA Confederations Cup. Catalyst for systematic cardiac screening.
2006	First mandatory PCMA implemented at FIFA World Cup, Germany.
2010	PCMA made compulsory for ALL FIFA competitions. Non-adherence becomes sanctionable.
2013	Snowden disclosures reveal Tempora (~21M GB/day) and INCENSER (~14B pieces/mo).
Jul 2020	FIFA Connect integration deadline for all 211 member associations.
Aug 2024	NIST FIPS 203/204/205 published. PQC standards finalized.
Mar 2026	Cain et al. / Oratomic (~26,000-qubit) and Google Research (<500,000-qubit) ECC-256 preprints. Physical-qubit estimates compress.
Jun 2026	**2026 FIFA World Cup kickoff (US/CAN/MEX). Peak cross-border medical-data concentration.**
Jan 2027	CNSA 2.0: new NSS acquisitions must be PQC-compliant.
2029	Google internal PQC migration deadline. Optimistic scenario for a CRQC.
2030 / 2035	NIST IR 8547 (initial public draft) deprecation (2030) and full disallowance (2035) targets for RSA/ECDSA.

APPENDIX G

WHY THE THESIS HOLDS IF THE TIMELINE SLIPS

A common objection to HNDL arguments is that the quantum timeline is uncertain and may extend well beyond current estimates. This appendix demonstrates that the thesis holds under substantially delayed timelines. The summary resilience table appears in Section 6.4; the full reasoning follows.

THE SENSITIVITY HORIZON TEST

- **Cardiac ECG data.** A cardiac anomaly detected in early adulthood remains medically relevant into old age. Horizon: 58+ years from collection.
- **Genetic predisposition markers.** Permanent. Horizon: lifetime of the individual.
- **Biometric elements, where present.** Cannot be reissued. Horizon: lifetime of the individual.
- **Concussion history.** Affects cognitive-health assessments for life, relevant in insurance, employment, and political contexts. Horizon: lifetime.

If a quantum computer capable of breaking classical encryption becomes available at any point before that data loses sensitivity, any encrypted copy collected in transit becomes decryptable. The thesis would be weakened only if (a) no such machine is built within the lifetime of the data subjects AND (b) no other cryptanalytic advance compromises the same algorithms during that period. Given the current trajectory across multiple independent programs, the likelihood of both holding for 50+ years appears low on present evidence, though it cannot be ruled out. This assessment may change as research evolves.

THE ASYMMETRY OF REGRET

The cost of migrating now and being wrong is manageable: stronger cryptography deployed, implementation cost incurred, no downside to data subjects. The cost of not migrating and being wrong is potentially catastrophic: lifetime-sensitive data for players across 211 nations permanently compromised, with no remediation possible. For cardiac ECG data, genetic markers, and biometric elements where present, the balance of evidence suggests the data's sensitivity horizon will exceed the period during which current encryption can be considered reliable. The remaining uncertainty is not whether this gap exists, but how wide it will be.

BACK MATTER

§ LEGAL, NON-RELIANCE & PUBLIC RELEASE NOTICES

DISCLAIMER

This material is provided as a public research report for informational purposes only and does not constitute legal, regulatory, compliance, investment, security, or other professional advice. This report does not allege that FIFA, any confederation, any member association, or any individual has experienced a data breach, or that any specific harvest-now-decrypt-later operation is targeting football data. It describes a structural risk inherent in the use of quantum-vulnerable cryptography to protect lifetime-sensitive medical and identity data across a global data infrastructure. Cost estimates, timeline projections, and hardware assessments reflect Qtonic Quantum's analysis of publicly available research and are subject to meaningful uncertainty. The March 2026 papers referenced are preprints that had not completed peer review as of publication.

NON-RELIANCE

No person or entity should rely on the contents of this report as a basis for any decision or action without obtaining independent professional advice specific to their circumstances. Qtonic Quantum Corp expressly disclaims any and all liability for actions taken or not taken based on any or all of the contents of this report. This report is not an offer, solicitation, or recommendation to purchase any product or service. Qtonic Quantum Corp offers commercial services in the field this report addresses. Readers should weigh that interest.

NAMED INDIVIDUALS

Individuals named in this report appear solely as publicly documented examples of athletes who later entered political or public life, drawn from public records and established reporting. This report makes no statement or implication that any named individual's data has been collected, intercepted, harvested, transmitted, stored, or decrypted, that any named individual's medical or biometric information is or was at risk, or that any named individual faces any specific or actual harm. References are illustrative of a general, documented pattern only. Their inclusion implies no criticism of any named individual. Biographical facts are drawn solely from public records.

NATURE OF STATEMENTS

Statements characterized as risk analysis, inference, projection, or structural assessment are expressions of opinion based on publicly available information, not assertions of fact. The evidence-category labels (C1 documented fact, C2 reasonable inference, C3 structural risk analysis) and the bounded language used throughout indicate the basis and confidence of each claim.

PUBLIC RELEASE & MEDIA USE

This report is approved for public distribution and may accompany press materials. Quotations attributed to the Qtonic Quantum Research Team or to Qtonic Quantum Corp in press materials are authorized only in the exact form approved in writing. Media inquiries may be directed to the contact details on the following page. Factual errors identified after publication will be corrected in subsequent versions and noted. Independent replication of the Appendix B search methodology is invited. Third-party names and marks, including FIFA, appear for identification and commentary only. Their use does not imply affiliation, sponsorship, or endorsement.

COPYRIGHT

REVISION HISTORY

REV J–N (11 June 2026 release): corrected the INCENSER source citation (App A); separated RSA-2048 and ECC-256 resource estimates by problem class and added the logical-versus-physical qubit distinction (§6.1, FIG.1); softened the Google preprint attribution pending author confirmation; added §6.5 (Global Risk Institute expert survey); marked NIST IR 8547 as initial public draft at each mention; scoped concentration language to identity and registration data through FIFA Connect, with medical and PCMA data moving through documented cross-border workflows; updated the cardiac-survey citation to its 2025 BJSM publication; bounded the intercontinental-traffic figure; updated issue metadata and the contact block for the 11 June 2026 public release; corrected §7 framing to national political office with one documented head-of-state case and retitled the §7.2 table to include national sports governance; bounded the §10 network-exposure sentence to linked records and flows subject to segmentation and access controls; reworded the §2 example grouping to public roles; widened the closing briefing offer to qualified institutional stakeholders. No correction changes the report's thesis or risk rating.

QTONIC QUANTUM

POST QUANTUM READY

CONTACT

Qtonic Quantum Corp

Miami, FL

+1 (866) 4-QTONIC

info@qtonicquantum.com · qtonicquantum.com