© OCT 2019 | IRE Journals | Volume 3 Issue 4 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV3I4-1719692

Toward an Integrated Conceptual Framework for Traceability and Chain-of-Custody Integrity in Pharmaceutical Distribution

OLUCHI BEATRICE ANEKE[1], ABIMBOLA CALEB ADESEMOYE[2]
[1] *Rivers State University, Port Harcourt, Nigeria*
[2] *Afe Babalola University (ABUAD), Ado-Ekiti, Nigeria*

Abstract- ***Modern pharmaceutical distribution moves medicines through long, multi-actor networks in which identity, provenance, custody, and condition can each be compromised. Regulatory and technical responses have advanced quickly, including serialization mandates, data exchange standards, good distribution practice guidance, and a growing body of work on distributed ledger and sensing technologies, yet they remain fragmented. Most concentrate on traceability, the technical capacity to follow a product through the chain, while the assurance that every custody transfer was authentic, authorized, and unbroken, here termed chain-of-custody integrity, is left implicit or treated as a separate concern. This paper argues that traceability and chain-of-custody integrity are distinct but interdependent constructs, and that integrity assurance requires their deliberate integration rather than the accumulation of point solutions. Drawing on supply chain traceability theory, the forensic conception of custody, and the contemporary regulatory and technical landscape, it proposes an integrated conceptual framework built on four integrity dimensions, namely identity, provenance, custody continuity, and condition, and a five-layer architecture spanning unique identification, event capture and data exchange, custody verification and authentication, condition and environmental integrity, and governance, trust, and accountability. Cross-cutting enablers of interoperability, security, and trust anchoring connect the layers, and the lower layers are shown to deliver traceability while the upper layers convert it into assurance. The framework is applied to a stylized distribution scenario to demonstrate how it locates integrity gaps that traceability-centric approaches leave hidden, and a set of propositions translates it into testable relationships. The framework offers regulators, supply chain actors, and technology providers a structured vocabulary for diagnosing where integrity is genuinely at risk and for designing systems in which traceability and custody assurance reinforce one another.***

Keywords: Pharmaceutical Distribution, Traceability, Chain of Custody; Supply Chain Integrity, Serialization, Provenance, Conceptual Framework

I. INTRODUCTION

Medicines are credence goods. A patient, and frequently a dispenser, cannot tell by inspection whether a product is authentic, correctly sourced, and properly handled. A tablet that has been counterfeited, diverted through an unauthorized channel, manufactured to substandard quality, or exposed to temperatures outside its labelled range often looks identical to a sound one. Whatever assurance a patient ultimately has therefore rests not on inspection at the point of use but on the integrity of the distribution system that delivered the product. That system has become longer, more global, and more intermediated over the past several decades. Active ingredients, finished goods, and packaging now routinely originate in different jurisdictions, and a single product may pass through manufacturers, contract packagers, primary and secondary wholesalers, repackagers, third-party logistics providers, brokers, and dispensers before reaching the person who takes it. Each transfer of physical possession and legal responsibility is an opportunity for error, abuse, or undetected degradation (Agbabiaka et al., 2019).

The scale of the resulting harm is now reasonably well documented, even if precise figures remain elusive because much of the activity is concealed. The World Health Organization has estimated that roughly one in ten medical products circulating in low and middle-income countries is substandard or falsified, and has built a global surveillance and monitoring system to gather reports of such products and quantify their public health and economic toll (World Health

Organization, 2017a, 2017b). Counterfeit incidents have been recorded across every major therapeutic class, and assessments of infiltration into the legitimate supply chain show that the problem is geographically widespread rather than confined to informal markets (Mackey & Liang, 2011; Mackey, Liang, York, & Kubic, 2015). The consequences range from therapeutic failure and the promotion of antimicrobial resistance to direct toxicity, avoidable death, and the erosion of confidence in health systems, alongside substantial economic losses to legitimate manufacturers and payers (Blackstone, Fuhr, & Pociask, 2014; Institute of Medicine, 2013).

These concerns have driven a sustained wave of regulatory and technical reform. Early instruments such as the United States Prescription Drug Marketing Act of 1987 introduced the idea of a drug pedigree, a documented account of each prior sale of a product, although in practice paper-based pedigrees proved difficult to standardize and enforce (U.S. Congress, 1987). Contemporary regimes are far more ambitious. The Drug Supply Chain Security Act, enacted as Title II of the Drug Quality and Security Act, mandates unit-level product identifiers, the exchange of transaction data at each change of ownership, verification obligations for suspect and illegitimate product, and a phased transition toward fully interoperable electronic tracing (U.S. Congress, 2013; Brechtelsbauer, Pennell, Durham, Hertig, & Weber, 2016). In the European Union, the Falsified Medicines Directive and its delegated regulation require a unique identifier and an anti-tampering feature on each prescription pack, verified through an end-to-end repository network, with the safety-feature obligations taking effect in February 2019 (European Parliament and Council, 2011; Commission Delegated Regulation (EU) 2016/161, 2016). In parallel, good distribution practice guidance has set custody-oriented expectations for the handling, storage, transport, and documentation of products in transit, including specific guidance for temperature-sensitive goods (World Health Organization, 2010, 2011).

Despite this progress, the conceptual foundations of the field remain underdeveloped in one important respect. Much of the regulatory and scholarly discourse frames the central problem as one of traceability, understood as the technical capacity to follow a product forward and backward through the chain. Traceability is necessary, but it is not the whole of integrity. A product can carry a perfectly authentic serial number and a complete electronic event history and still have been diverted, substituted, or mishandled at some point along its route. What such cases lack is not visibility but assurance: a guarantee that every transfer of custody was authorized, that the actors involved were accredited to perform it, that the unit was not altered, and that its physical condition was preserved throughout. This paper terms that property chain-of-custody integrity, treats it as conceptually distinct from traceability, and argues that the two must be integrated by design rather than pursued as separate programs.

The contribution of the paper is to articulate that integration. It distinguishes traceability from chain-of-custody integrity and identifies four integrity dimensions that any adequate account of distribution integrity must address. It then organizes the existing landscape of regulatory, identification, data-exchange, and technological responses into a five-layer architecture and shows how the layers must operate jointly to produce integrity rather than mere visibility. It applies the resulting framework to a stylized distribution scenario to demonstrate its diagnostic value, and it derives a set of propositions intended to render the framework testable in future empirical work. Throughout, the aim is conceptual clarification rather than the advocacy of any particular technology or regulatory model.

II. CONCEPTUAL FOUNDATIONS: TRACEABILITY AND CHAIN-OF-CUSTODY INTEGRITY

Traceability is a mature concept in supply chain and food safety scholarship, from which the pharmaceutical discussion implicitly borrows. A widely cited definition holds that traceability is the ability to access any or all information relating to that which is under consideration, throughout its entire life cycle, by means of recorded identifications (Olsen & Borit, 2013). Two capabilities are usually distinguished within this definition. Tracking refers to the ability to follow the downstream path of a unit from its origin toward the point of consumption, while tracing refers to the ability to reconstruct the upstream

history of a unit from any later point back toward its origin (Moe, 1998). A traceability system therefore couples the unique identification of a resource unit with the systematic recording of the events and transformations that unit undergoes, so that the recorded identifications can be queried in either direction (Mbonu et al., 2019b).

Beyond this basic structure, the literature characterizes traceability systems along several further attributes that are useful for the pharmaceutical case. Breadth refers to the amount of information recorded about each unit; depth refers to how far forward and backward the system can reach; and precision refers to the granularity at which a traceable unit is defined and the assurance with which one unit can be distinguished from another. The literature also distinguishes internal traceability, which concerns movements and transformations within a single organization, from external or chain traceability, which concerns the linking of records across organizational boundaries (Karlsen, Dreyer, Olsen, & Elvevoll, 2013). External traceability is the harder problem, because it depends on shared identification standards, agreed event semantics, and the willingness and technical capacity of independent actors to exchange data reliably. For pharmaceuticals, contemporary regulation has pushed granularity toward the individual saleable unit, which is the level at which counterfeiting and substitution typically occur, and has thereby pushed the field squarely into the domain of external traceability across many heterogeneous actors. The broader challenge of achieving end-to-end visibility and traceability across complex, multi-actor global supply chains has been examined in the wider supply chain literature.

What this body of work establishes is that traceability is fundamentally an epistemic property of a system. It concerns what can be known about a unit and its path. A system is more traceable when more information about origin, movement, and transformation can be reliably accessed, at finer granularity, across greater depth (Akomolafe & Agu, 2018; Dogbatsey et al., 2019). Crucially, traceability as ordinarily defined says little about whether the movements it records were legitimate. It assumes, rather than guarantees, that the recorded custodians were entitled to hold the product, and that the product they passed on was the product they had received, unaltered and intact. Traceability answers questions of the form what is this and where has it been, but not questions of the form was each step in that history authorized and was the product preserved along the way.

The concept of a chain of custody answers those second questions, and it originates in forensic science and evidentiary law, where it denotes the chronological documentation of the seizure, control, transfer, analysis, and disposition of physical evidence. Its purpose is to establish that an item presented at a later stage is the same item collected earlier, and that it was not tampered with, substituted, or contaminated in the interim. Three features of the forensic concept transfer directly to pharmaceutical distribution. First, custody is defined by responsibility rather than mere physical proximity: a custodian is an actor accountable for the integrity of the item while it is in their control, and accountability does not lapse simply because the item is handed to a carrier or held in a warehouse. Second, every transfer of custody is a discrete, documented event in which responsibility passes from one accountable actor to another, and the legitimacy of that event depends on both parties being authorized to participate in it (Dosunmu & Ogundele, 2019; Ladapo et al., 2018; Mbonu et al., 2019a). Third, the value of the chain lies in its continuity: a single undocumented, unauthorized, or unverified transfer breaks the chain and undermines confidence in everything downstream of the break, regardless of how complete the record appears.

Translated to distribution, chain-of-custody integrity is the assurance that responsibility for a pharmaceutical unit passed through an unbroken sequence of authorized and accountable custodians, that each transfer between them was legitimate and verifiable, and that the unit and its physical condition were preserved across each transfer. This is a normative and assurance-oriented property, in contrast to the epistemic character of traceability. Good distribution practice guidance gestures toward it when it assigns responsibilities for dispatch and receipt, requires that consignments be checked on receipt, and treats returns, recalls, and the handling of suspect products as matters of documented accountability (World Health Organization, 2010). Yet such guidance has historically been expressed as procedural obligation imposed on individual actors rather than as

a verifiable property of the distribution system considered as a whole. The difference matters: an actor can comply with its own procedures while the system-level chain is nonetheless broken at a handoff that no single actor was responsible for verifying end to end.

It is useful to introduce a third notion that bridges traceability and custody, namely provenance, understood not merely as a recorded path but as an authenticated history whose origin and each subsequent step can be vouched for. Provenance in this stronger sense is what links the epistemic and the normative: a path that is merely recorded supports traceability, whereas a path that is authenticated, in which each recorded step is bound to an accountable actor and cannot be silently altered, begins to support custody assurance. Trust is the correlative concept on the side of the actors. A distribution system does not trust a record in the abstract; it trusts records because it trusts the actors and authorities that created and vouched for them. This is why identity, provenance, and custody cannot be fully assured by technical recording alone, and why the governance that accredits actors and anchors trust is indispensable rather than ancillary. The framework developed below makes this dependence explicit by treating authenticated provenance and accountable custody as products of distinct layers that rest, ultimately, on a governing source of trust.

The distinction between the two constructs can be sharpened by considering cases in which they come apart. A product may be highly traceable yet lack custody integrity. Consider a genuine pack whose authentic unique identifier is recorded at every required point, but which is diverted into an unauthorized secondary channel, stored improperly during the diversion, and then reintroduced into the legitimate chain. The event record may be complete and the identifier genuine, so the unit is traceable in the ordinary sense, yet a custody transfer occurred outside the set of authorized actors and a handling failure went undetected. Conversely, a closed and tightly controlled distribution operation might enforce authorized handoffs through administrative means while lacking any systematic capacity to reconstruct unit-level history, so that custody is well controlled but visibility, and hence traceability, is poor. Neither configuration delivers integrity on its own. The relationship between the constructs is therefore one of necessary interdependence rather than equivalence. Traceability supplies the visibility, the recorded identifications and events, on which any judgment about custody must rest (Arumosoye & Obriki, 2019; Okonkwo et al., 2018b) one cannot verify that a chain of custody is unbroken without the capacity to observe the transfers that compose it. Custody integrity, in turn, supplies the assurance that the observed chain is legitimate. Integrity in distribution is the property that emerges when the two are designed to operate jointly, and it is the central concern of the framework developed below.

III. THE PHARMACEUTICAL DISTRIBUTION ENVIRONMENT

Pharmaceutical distribution is multi-echelon and rarely linear, and understanding its structure is a precondition for understanding where integrity is at risk. Finished products typically move from a manufacturer or its contracted packager to primary wholesalers, and from there to secondary wholesalers, hospital and retail pharmacies, dispensing physicians, and other points of care (Aminu-Ibrahim et al., 2019; Ogbete et al., 2019). Superimposed on this forward flow are several structural features that complicate custody in ways that simple linear depictions of the supply chain obscure.

The first is the separation of custody from ownership. Third-party logistics providers take physical possession of products, and assume responsibility for their condition and security, without taking legal title. Brokers, conversely, may arrange transactions and take title without ever physically handling the goods. This decoupling means that the question of who is accountable for a unit at a given moment cannot be answered by tracking either ownership or physical location alone; it requires an explicit account of custody as a distinct relation (Akomolafe & Agu, 2019a; Okonkwo et al., 2019). The second feature is transformation of the saleable unit. Repackagers and relabellers alter the unit and its identifiers, and they re-establish the aggregation relationships that link items to cases and cases to pallets. Each such transformation is a point at which identity and provenance must be carried forward correctly, and at which they can be corrupted, whether accidentally or deliberately.

The third feature is reverse logistics. Returns, whether of saleable stock or of product withdrawn for quality reasons, reintroduce units into the chain after a period during which their custody and condition were outside the direct control of the parties who will now handle them. Recalls impose the additional demand that specific units be located and removed quickly and completely. Saleable returns are a particular concern, because a returned unit that is restocked and resold carries with it whatever happened during its absence, which the receiving party may have no means to verify (Agbabiaka et al., 2019; Okonkwo et al., 2018b). The fourth feature is the existence of secondary markets, parallel trade, and grey markets that adjoin the legitimate chain. Parallel trade, legitimate in some regions, exploits price differences across markets and creates additional, harder-to-monitor pathways along which units travel; grey-market and diversion activity exploits the same price differences illegitimately. Because the legitimate and illegitimate pathways run alongside one another and exchange units at their boundaries, the points where they meet, often returns and the secondary market, are recurrently identified as the principal points of entry for falsified and diverted product (Mackey et al., 2015; Institute of Medicine, 2013).

The persistence of diversion and grey-market activity is, at bottom, a matter of incentives, and recognizing this clarifies why purely technical countermeasures are incomplete. Where the same product commands materially different prices across markets, customer classes, or reimbursement regimes, an arbitrage opportunity exists, and some actors will be drawn to exploit it by moving product out of its intended channel and reintroducing it elsewhere at a higher price. Identification and event capture make such movement more visible after the fact, but visibility deters only to the extent that an accountable authority can act on it; absent accreditation of who may take custody and consequences for unauthorized transfers, a complete event trail may simply document a diversion without preventing it. This is why custody continuity is properly understood as a governance problem as much as a technical one, and why the framework developed below places the accreditation of custodians and the assignment of liability at its governing layer rather than treating them as adjuncts to the data systems (Akomolafe & Agu, 2019c; Okonkwo et al., 2019).

A fifth feature, cutting across the others, is the physical sensitivity of many products. Vaccines, biologics, insulin, and a growing range of advanced therapies must be kept within defined temperature ranges, and sometimes within humidity, light, and shock constraints, throughout storage and transport. The guidance developed for time and temperature-sensitive pharmaceutical products reflects the operational difficulty of maintaining these conditions across multiple custodians and modes of transport, and the consequences of failing to do so (World Health Organization, 2011). Condition is distinctive among the concerns of distribution because a condition failure can occur on a unit whose identity and provenance are entirely sound, and it leaves no trace in any record that captures only identity and movement.

Each of these features multiplies the number of custody transfers and the heterogeneity of the actors involved, and with them the number of points at which custody can be broken or condition compromised. The structure of the network is therefore itself a determinant of integrity risk. It also explains why distribution, rather than manufacturing, is the critical locus for integrity. Manufacturing operates under comparatively concentrated regulatory oversight and quality management, within facilities that are licensed and inspected. Distribution, by contrast, is where ownership and custody change hands repeatedly, across many actors and jurisdictions, and where the legitimate and illegitimate supply chains most often intersect. Improving integrity is, to a substantial degree, a problem of distribution design, and frameworks for integrity should take the multi-custodian transfer, rather than the production batch, as their primary unit of analysis (Aminu-Ibrahim et al., 2018; Obogo et al., 2019c; Obriki & Arumosoye, 2018; Ogbete et al., 2019).

IV. A STRUCTURED TYPOLOGY OF INTEGRITY THREATS

The threats to distribution integrity are diverse, but they can be organized coherently by the integrity dimension each primarily attacks. This organization is more than taxonomic convenience; it anticipates the framework developed later, in which each dimension

is served by particular layers of a distribution system, and it makes clear why no single countermeasure can address the whole problem (Akomolafe & Agu, 2019b; Dosunmu & Ogundele, 2019).

Counterfeiting and falsification attack identity and provenance. An illegitimate unit is presented as a genuine one, whether by imitating its appearance, by cloning a genuine identifier onto false product, or by manufacturing product with no or incorrect active ingredient and packaging it to pass as authentic. These threats target the correspondence between a unit and what its label and identifier assert about it, and they target the authenticity of the history that would otherwise vouch for it. Substandard product attacks identity in a related but distinct way: the unit may be genuinely produced by the named manufacturer yet fail to meet quality specifications, whether through manufacturing defect or subsequent degradation, so that it is not, in substance, what its label warrants (Aminu-Ibrahim et al., 2019; Ogbete et al., 2019).

Diversion attacks custody continuity. A genuine, sound unit is moved through an actor or channel outside the authorized set, typically to exploit price differences across markets or customer classes, and is then often reintroduced into the legitimate chain. The physical product may be entirely authentic, which is precisely why diversion is invisible to countermeasures that check only identity; what has failed is the requirement that custody pass only through authorized, accountable actors (Okonkwo et al., 2019; Obogo et al., 2019b). Theft, including cargo theft, similarly severs custody and reintroduces units whose intervening handling and condition cannot be verified. Documentary falsification attacks provenance directly, by forging or altering the transaction records, certificates, and pedigrees on which traceability depends, so that a corrupted history is made to appear sound (Akomolafe & Agu, 2019b; Dogbatsey et al., 2019; Mbonu et al., 2019b). Tampering attacks identity and condition together, by interfering with the unit or its packaging in ways that may or may not be detectable after the fact.

Finally, improper storage and transport attack condition alone. A temperature excursion, a humidity breach, or rough handling can render a unit unsafe or ineffective without disturbing its identity or its recorded provenance in any way. This is the class of threat most often overlooked by traceability-centric thinking, because it cannot be detected by any system that records only what a unit is and where it has been. A serialized pack with a complete and authentic event history can nonetheless have spent hours outside its permitted temperature range, and nothing in the identifier or the event record will reveal it (World Health Organization, 2011).

Two observations follow from this typology and motivate the framework. The first is that the threats are not reducible to a single failure mode and do not all manifest in the same part of a distribution system. Some appear as anomalies in identification or event data; others, such as diversion of an authentic unit or a cold-chain excursion on an otherwise sound product, are invisible to systems that record only identity and movement. The second is that the threats often combine. Diverted product may be stored improperly during its time outside the legitimate chain and may acquire falsified documentation before reintroduction, so that a single illegitimate episode attacks custody continuity, condition, and provenance at once. An adequate framework must therefore span all of the dimensions that the threats collectively target, and must connect the mechanisms that address each, rather than treating them as separate compliance exercises (Agbabiaka et al., 2019; Obogo et al., 2019c; Obriki & Arumosoye, 2018).

V. EXISTING APPROACHES AND THEIR LIMITATIONS

Responses to distribution integrity have developed along several largely parallel tracks: regulatory and governance instruments, identification and serialization standards, data exchange and event capture, and a growing set of emerging technologies (Akomolafe & Agu, 2018; Dosunmu & Ogundele, 2019; Mbonu et al., 2018). Each track is reviewed in turn, after which the fragmentation that results from treating them in isolation is characterized.

5.1 Regulatory and governance instruments

Regulatory instruments establish the obligations and the institutional context within which integrity is pursued, and they reveal, on inspection, markedly different conceptions of where integrity is generated (Akomolafe & Agu, 2019c; Dogbatsey & Ebhojie,

2018). The pedigree requirements introduced by the Prescription Drug Marketing Act represented an early, document-centric attempt to attach a custody history to a product, but the difficulty of standardizing and authenticating paper pedigrees across many states and actors limited their effectiveness (U.S. Congress, 1987). The Drug Supply Chain Security Act replaced this patchwork with a national, phased program. Its early phases required the exchange of transaction information, transaction history, and a transaction statement at each change of ownership, initially at the lot level. Subsequent phases required serialization of product at the unit level through a standardized product identifier, and verification processes for suspect and illegitimate product, including the verification of saleable returns before they may be resold. Its culminating phase requires interoperable, electronic, unit-level tracing across trading partners (U.S. Congress, 2013; Brechtelsbauer, Pennell, Durham, Hertig, & Weber, 2016). The model is, in lineage and emphasis, transaction-centric: assurance is generated at each documented change of ownership between trading partners.

The European Falsified Medicines Directive took a complementary but architecturally different path. It pairs a unique identifier and an anti-tampering device on each pack with an end-to-end verification model: packs are recorded at the point of manufacture into a central European Hub operated by the European Medicines Verification Organisation, the data is distributed to national repositories run by national verification organisations, and packs are verified and decommissioned at the point of dispensing, with risk-based verification at intermediate points (European Parliament and Council, 2011; Commission Delegated Regulation (EU) 2016/161, 2016). The European model is, in emphasis, end-point-centric: assurance is generated principally by verifying pack authenticity where the product enters and leaves the system, rather than by documenting every intervening transaction. The contrast is instructive because each model is strong where the other is weaker. A transaction-centric model captures custody handoffs but can struggle with completeness at the endpoints, while an end-point-centric model verifies authenticity at dispensing but records less about the legitimacy of intervening custody.

Beyond these two influential regimes, a growing number of jurisdictions have introduced serialization and verification requirements, producing a varied global landscape rather than a single harmonized system. India operates a drug authentication and verification application for the upload and checking of serialization data, with a strong emphasis on exports; Brazil has developed a national medicines control system under its health regulator that requires serialization and real-time reporting to a government database; Russia operates a centralized system requiring cryptographic codes; and China has long required the transmission of supervision data to government-operated platforms. In Africa, national regulators and regional bodies have advanced traceability strategies aimed at supply chain visibility against substandard and falsified products, supported by international coordination. The World Health Organization, for its part, contributes both custody-oriented good distribution practice guidance and a global surveillance and monitoring system for substandard and falsified products, and supply chain security management standards address the procedural and organizational dimension of security more generally (World Health Organization, 2010, 2017b; International Organization for Standardization, 2007). What this landscape demonstrates is that even the regulatory layer is internally fragmented in its conception of what integrity requires, divided between transaction-centric and end-point-centric models, varied in granularity and architecture across jurisdictions, and uneven in the degree to which any of these instruments addresses condition as opposed to identity and provenance (Akomolafe & Agu, 2019a, 2019c).

5.2 Identification and serialization standards

Underlying most modern schemes is a common stratum of identification standards, predominantly those maintained by GS1. A Global Trade Item Number identifies a product type, a Serial Shipping Container Code identifies an individual logistics unit such as a case or pallet, and a Global Location Number identifies parties and physical locations (GS1, 2018). Unit-level traceability is achieved by serializing the trade item, combining the trade item number with a unique serial number, and encoding it together with batch and expiry data in a two-dimensional data

carrier, commonly a GS1 DataMatrix, that can be read at speed on a packaging line and at points of dispensing. Aggregation relationships, which record that particular items are contained in a particular case and that particular cases are loaded on a particular pallet, allow a custodian to infer the contents of a higher-level unit, and to update the status of many items at once, without opening the unit, provided the parent-child links are accurately created and maintained through every transformation (Ogbete et al., 2019; Okonkwo et al., 2018b).

The identification layer answers the question of what a unit is, and it is a precondition for everything built above it; without a reliable, unique, machine-readable identity, there is nothing to trace, verify, or attest. But it is important to be precise about what this layer does not do. A serial number, however well constructed and encoded, records nothing about where the unit has been, who has held it, whether each handoff was authorized, or whether the unit was kept within its required conditions. Serialization establishes the referent; it does not, in itself, establish provenance, custody continuity, or condition. Treating serialization as equivalent to integrity, a common rhetorical slippage, is the first and most basic form of the fragmentation this paper diagnoses.

5.3 Event capture and data exchange

Visibility across organizational boundaries depends on a shared way of capturing and exchanging the events in a unit's life. The Electronic Product Code Information Services standard provides such a vocabulary, representing events in terms of what objects were involved, when the event occurred, where it took place, and the business context in which it happened, the last expressed through a controlled vocabulary of business steps and dispositions (GS1, 2016). The standard distinguishes several event types, including object events that record observations of units, aggregation events that record the association of units into higher-level containers and their later disaggregation, transaction events that link units to business transactions such as purchase orders, and transformation events that record the consumption of inputs and the production of new outputs, as in repackaging. Standardized events of these kinds make it possible, in principle, for independent actors to contribute to and query a common picture of a unit's path (Mbonu et al., 2019b).

The harder questions at this layer are architectural rather than semantic. Event data may be held in centralized repositories, in fully distributed stores queried on demand, or in semi-distributed arrangements that combine a directory with distributed detail (Dosunmu & Ogundele, 2019; Ladapo et al., 2019). Authenticity may be checked by pushing event data forward with the product, so that each recipient holds the history, or by pulling a verification response from the party that generated an identifier, as in the verification of saleable returns through a routing service that locates and queries the responsible manufacturer. Each arrangement embodies trade-offs among confidentiality, since trading partners are often reluctant to expose commercially sensitive movement data, scalability, since unit-level events across a national or global market generate enormous data volumes, and the difficulty of locating the relevant records, sometimes called the lookup or directory problem. The data exchange layer is what turns identification into traceability; it converts a collection of identifiers into a navigable history. But in its standard form it remains a record of movement rather than a verification of the legitimacy of custody. It can faithfully record that a unit moved from one party to another without establishing that the receiving party was authorized to take custody or that the transferring party was entitled to release it (Dosunmu & Ogundele, 2019; Ladapo et al., 2018; Mbonu et al., 2018, 2019a).

5.4 Emerging technologies

A substantial recent literature explores technologies that promise to strengthen one or more aspects of integrity. Distributed ledger and blockchain approaches have attracted particular attention as a means of maintaining a shared, tamper-evident record of provenance across actors who do not fully trust one another and who are reluctant to cede control to a single central intermediary. Reviews have catalogued their potential alongside other digital tools for combating falsified medicines (Mackey & Nayyar, 2017), and specific proposals include shared provenance ledgers for the pharmaceutical chain (Bocek, Rodrigues, Strasser, & Stiller, 2017), blockchain-based product ownership management designed to make each change of ownership explicit

and verifiable rather than merely recorded (Toyoda, Mathiopoulos, Sasase, & Ohtsuki, 2017), and broader explorations of distributed ledgers for healthcare supply chain management (Clauson, Breeden, Davidson, & Mackey, 2018). The appeal of these approaches lies less in the ledger as such than in the properties they can confer: tamper evidence, shared visibility without a single owner, and the possibility of binding cryptographic attestations to events.

A parallel strand of work addresses condition rather than identity, using networked sensors to monitor temperature and other handling parameters in transit and to bind the resulting data to the consignment, an approach especially relevant to time and temperature-sensitive products and sometimes combined with ledger-based recording so that condition data inherits the same tamper evidence as provenance data (World Health Organization, 2011; Bocek et al., 2017). Authentication technologies form a third strand, including overt features that a user can check, covert features detectable only with specialized tools, forensic markers, and the mass-serialization verification performed when a pack is scanned at the point of dispensing. Each of these technologies is valuable, and each is frequently presented, in vendor and sometimes in scholarly discourse, as a comprehensive solution. In fact each addresses a specific facet of the problem. A shared provenance ledger improves the trustworthiness of the event record but does not, in itself, ensure that a given custodian was authorized or that a product was kept cold. Sensor-based monitoring assures condition but says nothing about identity or the legitimacy of a transfer. Point-of-dispensing verification confirms authenticity at the endpoint but provides limited assurance about the intervening custody (Aminu-Ibrahim et al., 2018; Ogbete et al., 2019). The technologies are best understood not as competing solutions but as mechanisms that serve different dimensions and layers, a perspective the framework makes explicit.

5.5 The fragmentation problem

Viewed together, these tracks reveal a recurrent pattern. Each addresses a slice of the integrity problem, and each tends to be evaluated against the objective internal to its own track: serialization against the completeness and quality of identification, data exchange against the completeness of the event record, regulation against procedural compliance, and emerging technologies against the specific capability they introduce. What is missing is an integrating conception that connects identity, provenance, custody continuity, and condition under a common governance, and that makes explicit how the technical layers must operate jointly to yield assurance rather than mere visibility. The consequence of this fragmentation is not merely conceptual untidiness. It produces systems that are strong in one dimension and silently weak in another: richly serialized but blind to diversion, or fully sensored but unable to verify the legitimacy of a handoff (Akomolafe & Agu, 2019a; Okonkwo et al., 2019). It deprives regulators and designers of a shared vocabulary for locating where, in a given distribution system, integrity is actually at risk. And it encourages the rhetorical equation of traceability with integrity, which obscures precisely the gaps that the threats of diversion and condition failure exploit. The next section proposes an integrating conception intended to close these gaps.

VI. AN INTEGRATED CONCEPTUAL FRAMEWORK

At the conceptual core of the framework are four dimensions that together constitute distribution integrity. Identity integrity is the property that a unit is what it claims to be: the saleable item corresponds to its declared product, strength, batch, and identifier, and is neither counterfeit nor substandard relative to its label. Provenance integrity is the property that the unit's origin and recorded path are authentic and complete, so that its history can be trusted and has not been fabricated or selectively altered. Custody continuity is the property that responsibility for the unit passed through an unbroken sequence of authorized, accountable custodians, with each transfer between them legitimate and verifiable. Condition integrity is the property that the unit was handled and stored within its required parameters throughout, so that its physical quality was preserved. Chain-of-custody integrity, as used in this paper, is the conjunction of these four dimensions sustained across the entire distribution path. The dimensions are partly independent: a unit can satisfy identity and provenance while failing condition, or satisfy identity and condition while failing custody continuity through

© OCT 2019 | IRE Journals | Volume 3 Issue 4 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV3I4-1719692

diversion, or carry an authentic identity on a falsified history. Because they are partly independent, overall integrity is bounded by the weakest dimension present at any echelon, in the manner of a chain whose strength is that of its weakest link (Akomolafe & Agu, 2019b; Arumosoye & Obriki, 2019; Mbonu et al., 2018).

These four dimensions are operationalized through five functional layers. The layers are ordered so that each depends on those below it, and so that the lower two correspond broadly to traceability while the upper three add the assurance that converts traceability into chain-of-custody integrity. The first layer, unique identification and serialization, establishes the referent: a unique, machine-readable identity for each traceable unit, together with the aggregation relationships among units. The second layer, event capture and data exchange, records and shares standardized events as the unit moves and is transformed, supplying visibility across organizational boundaries. The third layer, custody verification and authentication, turns that visibility into assurance: at each transfer, the receiving custodian verifies the authenticity of the unit and the legitimacy of the transferring party, and an attestation of the handoff is created that accountable parties cannot later repudiate. The fourth layer, condition and environmental integrity, captures handling data such as temperature and binds it to the unit, so that condition can be assured alongside identity and provenance. The fifth layer, governance, trust, and accountability, defines the roles, accreditation, liabilities, audit rights, and dispute resolution that give the technical layers their authority and that establish, in the first place, who is entitled to act as a custodian. Table 1 summarizes the layers, the dimensions they primarily serve, and the failure that results when each is absent.

Table 1. The five-layer architecture and the integrity dimensions it serves.

Layer	Function and mechanisms	Primary dimension served	Failure mode if absent
Identification and serialization	Unique unit identifiers, data carriers, aggregation (GTIN, SSCC, GLN, DataMatrix)	Identity	No referent to trace or verify
Event capture and data exchange	Standardized events and repositories (EPCIS); push or pull verification	Provenance	Path unknown; no visibility
Custody verification and authentication	Authenticated, attested handoffs between accredited custodians; non-repudiation	Custody continuity	Diversion and substitution go undetected
Condition and environmental integrity	Sensing and binding of handling data (temperature, tamper evidence) to the unit	Condition	Handling failures invisible
Governance, trust, and accountability	Accreditation of actors, roles, liability, audit, dispute resolution	All (binds the chain)	Attestations lack authority

Three enablers cut across all five layers and are conditions of their joint operation rather than layers in their own right. Interoperability, grounded in shared standards for identification and event semantics, is what allows independent custodians to participate in a common system; without it, each actor's records remain islands and external traceability collapses, however sophisticated any individual actor's internal systems may be. Security and cryptography provide the means by which the attestations created at the custody verification layer, and the condition records created at the condition layer, can be made authentic and non-repudiable, through mechanisms such as digital signatures and verifiable credentials that bind a claim to an identified, accountable actor (Ladapo et al., 2018; Mbonu et al., 2019b). Trust anchoring is the institutional and technical foundation that establishes which actors and which roots of authority are to be trusted: the accreditation of custodians, the credentialing of parties entitled to generate or verify identifiers, and the roots of trust against which signatures and attestations are validated (Dosunmu &

Ogundele, 2019). It is within this cross-cutting role, rather than as a distinct layer, that distributed ledger approaches are best located: they offer one possible substrate for trust anchoring and tamper-evident provenance, valuable where no single trusted intermediary is acceptable to all parties, but neither necessary nor sufficient for integrity by themselves.

The framework's central claim concerns how the layers combine to produce integrity. Identification and event capture, the lower two layers, deliver traceability: together they make it possible to know what a unit is and where it has been. This is necessary but not sufficient for integrity, because a complete and authentic event record can still describe an illegitimate journey, as the diversion case makes clear. Custody verification, the third layer, is the pivot of the framework. By requiring that each transfer be authenticated and attested by accredited custodians, it converts the passive event record into an active assurance that the recorded chain is legitimate and unbroken. A handoff is no longer merely observed; it is verified and vouched for by parties who can be held accountable. Condition integrity, the fourth layer, extends assurance from the unit's identity and path to its physical state, addressing the class of threats that leave identity and provenance untouched. Governance, the fifth layer, supplies the authority without which attestations are merely claims: it defines who may be a custodian, what their obligations and liabilities are, and how the records are audited and disputes resolved (Akomolafe & Agu, 2019a, 2019c; Dogbatsey et al., 2019). Chain-of-custody integrity, in this account, is an emergent property that exists only when the assurance layers operate on top of the traceability layers and within a governing institutional frame. Investment in traceability alone, however advanced, raises visibility without guaranteeing integrity, which is the precise failure that the fragmentation of existing approaches tends to produce.

A brief illustration of a single custody transfer makes the integrative logic concrete. When a consignment passes from a wholesaler to a hospital pharmacy under the framework, the receiving pharmacy reads the unit identifiers and their aggregation relationships, drawing on the identification layer. It queries the event history to confirm that the recorded path is consistent and complete, drawing on the data exchange layer. It verifies that the transferring wholesaler is an accredited custodian entitled to release the product, and it records an attestation, signed in a way that neither party can later repudiate, that custody has passed, drawing on the custody verification layer and on the security and trust-anchoring enablers (Dosunmu & Ogundele, 2019). It checks the bound condition record to confirm that the consignment remained within its permitted temperature range throughout transit, drawing on the condition layer. And the authority for each of these checks, the accreditation of the wholesaler, the meaning of the attestation, and the recourse available if a discrepancy is found, derives from the governance layer (Dogbatsey & Ebhojie, 2018; Okonkwo et al., 2019). A break in any one of these, an unverifiable identifier, a gap in the history, an unaccredited transferor, a condition excursion, or an absence of governing authority, is a break in integrity, even if all the others are sound. This is the sense in which integrity is bounded by the weakest dimension at the handoff.

Several relationships follow directly from this logic and are stated here as propositions to be tested in future empirical work. First, traceability infrastructure, comprising the identification and event-capture layers, is necessary but not sufficient for chain-of-custody integrity; integrity additionally requires the assurance layers of custody verification, condition integrity, and governance. Second, chain-of-custody integrity increases with the proportion of custody transfers that are authenticated and attested by accredited actors, rather than merely recorded (Akomolafe & Agu, 2019a). Third, system integrity is bounded by the weakest of the four integrity dimensions present at any echelon. Fourth, the marginal integrity benefit of unit-level serialization rises with the maturity of the verification and governance layers above it, so that the same serialization investment yields more integrity in a system with strong custody verification than in one without it. Fifth, condition integrity is independent of identity and provenance integrity and must be assured separately, since serialization and event capture do not detect handling failures (Arumosoye & Obriki, 2018). Sixth, governance mechanisms that assign liability and enable audit increase actor compliance with custody attestation requirements (Akomolafe & Agu, 2018; Obogo et al., 2019a). Seventh, interoperability across custodians moderates the relationship between local

© OCT 2019 | IRE Journals | Volume 3 Issue 4 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV3I4-1719692

traceability investment and system-level integrity, so that in low-interoperability settings local investment yields limited system-level gains. Table 2 maps the principal threats to the dimensions they attack and to the layers that detect or prevent them, and in doing so summarizes how the framework connects the threat typology of Section 4 to the architecture proposed here.

Table 2. Mapping of principal threats to integrity dimensions and to the layers that address them.

Threat	Dimension attacked	Layer that detects or prevents it
Counterfeiting / falsification	Identity, provenance	Identification; event capture; custody verification
Substandard product	Identity	Identification; governance (quality accountability)
Diversion	Custody continuity	Custody verification; governance (accreditation)
Theft	Custody continuity, condition	Custody verification; condition integrity
Documentary falsification	Provenance	Event capture; security (non-repudiation)
Tampering	Identity, condition	Identification (anti-tamper); condition integrity
Improper storage / transport	Condition	Condition integrity (sensing and binding)

VII. APPLYING THE FRAMEWORK: AN ILLUSTRATIVE DIAGNOSTIC

The value of a conceptual framework is partly in what it allows one to see. To demonstrate its diagnostic use, consider a stylized distribution system, described in general terms rather than with reference to any actual organization or data. A manufacturer serializes its product at the unit level and records manufacture events; primary and secondary wholesalers exchange standardized movement events as the product changes hands; and a hospital pharmacy verifies pack authenticity at the point of dispensing. By the standards of much current practice, this system would be regarded as advanced (Agbabiaka et al., 2019; Okonkwo et al., 2018b). Applying the four dimensions and five layers, however, reveals where its integrity nonetheless depends on assumptions that are not actually assured.

On the dimensions of identity and provenance, the system is strong: units are uniquely identified, their manufacture is recorded, their movement is captured in standardized events, and their authenticity is checked at dispensing. The identification and event-capture layers are mature, and the threats of overt counterfeiting and incomplete history are well addressed. The weaknesses appear on the dimensions the traceability layers do not reach. Consider custody continuity. The system records that product moved from the primary to the secondary wholesaler, but if it does not verify that the secondary wholesaler was an accredited custodian entitled to receive it, nor capture a non-repudiable attestation of the handoff, then a diversion in which authentic product is routed through an unauthorized actor and reintroduced may leave a plausible-looking event trail (Dogbatsey et al., 2019; Mbonu et al., 2019b; Okonkwo et al., 2019). The custody verification layer is absent or weak, and the governance layer has not established and enforced who may take custody. The framework locates the gap precisely: it is not a failure of identification or of data capture, both of which functioned, but a failure of the assurance layer that those lower layers were mistakenly assumed to provide.

Consider next condition. If the product is temperature-sensitive but the system binds no condition record to the consignment, then a cold-chain excursion during transit between wholesalers will be entirely invisible (Arumosoye & Obriki, 2018; Sunday et al., 2019). The pack will scan as authentic at dispensing, its history will appear complete, and yet its physical integrity may be compromised. Again, the framework identifies the missing element as the condition layer, independent of the identity and provenance assurances that the system does provide. Finally, consider the handling of saleable returns. A returned unit

reintroduced without verification of its intervening custody and condition imports an unverified gap into an otherwise sound chain; the framework shows that closing this gap requires not more identification but custody verification and condition assurance applied to the return as rigorously as to forward flow, under a governance regime that makes such verification obligatory.

The illustration is deliberately schematic, but it demonstrates the framework's central practical claim. A system can be advanced on the traceability layers and still be silently weak on custody continuity and condition, precisely because those dimensions are served by layers that traceability-centric design tends to omit. The framework does not by itself remedy such gaps, but it makes them visible and nameable, which is the precondition for remedying them. It also clarifies that the appropriate response is not invariably more technology of the kind already deployed, but the addition of the specific assurance layer that the unaddressed dimension requires (Akomolafe & Agu, 2018; Obogo et al., 2019c).

VIII. DISCUSSION AND IMPLICATIONS

The framework carries implications for the principal participants in pharmaceutical distribution, and it reframes several familiar debates. For regulators, it suggests that a regime should be evaluated not only by the traceability it mandates but by the integrity dimensions it actually assures. A scheme that requires serialization and transaction documentation strengthens identity and provenance, but unless it also requires authenticated custody transfers and addresses condition, it leaves custody continuity and condition under-assured. The contrast between transaction-centric and end-point-centric models becomes, in this light, a contrast in which assurance layers each model emphasizes and which it leaves implicit, and the framework provides a vocabulary for recognizing and closing the gap each leaves. The framework also underscores the importance of governing returns and the secondary market explicitly, since these are the points at which custody continuity most often breaks, yet they are frequently treated as exceptions to a design built around forward flow. A regulator that mandates verification of saleable returns is, in the framework's terms, extending the custody verification layer to the reverse-logistics paths where it is most needed.

For manufacturers, wholesalers, and logistics providers, the framework reframes the handoff as the primary object of design. Rather than treating serialization and good distribution practice as separate compliance streams, with serialization owned by packaging and information technology functions and good distribution practice owned by quality and operations, actors can design each change of custody as a single attested event that simultaneously updates the traceability record, verifies the authenticity of the unit and the legitimacy of the counterparty, and binds the relevant condition data. This integrated conception of the handoff is particularly consequential for third-party logistics providers, whose custody is separated from ownership and who therefore need a way to assume and discharge custodial responsibility explicitly, and for repackagers, who must re-establish identity and aggregation relationships in a verifiable way that carries provenance forward across the transformation. Reverse logistics deserves the same treatment as forward flow, since a return that is not handled as an attested custody event is a latent break in the chain that the receiving party cannot detect (Agbabiaka et al., 2019; Okonkwo et al., 2018a).

For technology providers and standards bodies, the framework implies that the most valuable work lies not within any single layer but at the interfaces between them, and especially in building custody verification and attestation on top of the existing identification and event-capture standards rather than alongside them. Event semantics can be extended so that an attested custody transfer, and a bound condition record, become first-class constructs rather than information carried informally or in parallel systems. Distributed ledger technologies are best positioned as a substrate for trust anchoring and tamper-evident provenance, deployed where the absence of an acceptable central intermediary makes shared, tamper-evident records valuable, rather than as ends in themselves or as substitutes for the governance that gives attestations their authority (Ladapo et al., 2019; Mbonu et al., 2018). Interoperability, in this account, must extend not only to the recording of movement but to these assurance functions, since an attestation that

cannot be interpreted and trusted across organizational boundaries provides little system-level assurance.

The framework is also intended to remain meaningful across very different infrastructural settings, and this has implications for equity. In well-resourced systems, all five layers can be richly instrumented with automated capture, networked sensing, and sophisticated cryptographic attestation. In lower-resource settings, where the burden of falsified and substandard medicines is heaviest, the same conceptual structure can guide lighter-weight implementations: mobile-based authentication at the point of dispensing, simplified custody attestation that nonetheless records who took responsibility and when, and targeted condition monitoring focused on the most sensitive products rather than the entire catalogue. The value of the framework in such contexts is that it makes explicit which integrity dimensions a lightweight implementation does and does not assure, so that residual risk is understood and consciously accepted rather than hidden behind the presence of some traceability capability. A system that can authenticate identity but cannot verify custody or condition is not thereby worthless; it is simply assuring two dimensions and not the other two, and the framework allows that to be stated plainly.

Several implementation challenges temper these implications and merit acknowledgement. The data volumes generated by unit-level events across a national or global market are very large, and the systems that capture, exchange, and verify them must scale accordingly. Trading partners have legitimate concerns about the confidentiality of movement data, which can reveal commercially sensitive information about volumes and relationships, and any custody verification scheme must reconcile verifiability with confidentiality. The broader literature on enterprise data protection, secure implementation, and regulatory risk modeling bears directly on this challenge, since the event and movement data exchanged among custodians is itself sensitive, regulated enterprise data that must be classified, protected, and governed for compliance. Interoperability depends on governance arrangements, standard-setting, accreditation, and dispute resolution, that are as much institutional as technical and that may be difficult to establish across jurisdictions with different legal traditions and regulatory capacities (Aliliele et al., 2024a; Mbonu et al., 2019b). And the addition of assurance layers imposes costs that must be justified by the integrity they deliver, which is why the proportionality principle, matching the assurance sought to the risk, is built into the framework rather than treated as an afterthought.

A further task, intermediate between the conceptual framework and its empirical test, is measurement. If integrity is bounded by the weakest of four dimensions, then assessing a distribution system requires some means of gauging each dimension and the maturity of each layer. Identity assurance might be approached through the coverage and reliability of authentication at the relevant points; provenance through the completeness and tamper resistance of the event history; custody continuity through the proportion of transfers that are verified and attested by accredited actors rather than merely recorded; and condition through the coverage of monitoring for products that require it and the rate at which excursions are detected and acted upon. The maturity of each layer might in turn be characterized on an ordinal scale running from absent, through present but not interoperable, to interoperable and governed. Such measures are not proposed here in finished form, and developing and validating them is itself a research undertaking, but identifying the dimensions and layers as the objects to be measured is a precondition for moving from the rhetoric of traceability toward an evidence-based account of integrity. It also yields a practical diagnostic: a system that scores well on the lower layers and poorly on the upper ones is, in the framework's terms, traceable but not assured, and a measurement of that kind makes the gap explicit rather than leaving it to be discovered when a failure occurs.

Finally, the limitations of the contribution should be stated plainly. The framework is conceptual and has not been empirically validated; its propositions are offered as hypotheses to be tested rather than as established findings. The four dimensions and five layers are analytical abstractions, and real systems will blur the boundaries between them, combining functions in single technologies or splitting a single layer across several. The framework is deliberately technology-neutral, which is a strength for generality and longevity but means that it does not prescribe

specific implementations or adjudicate among competing technical standards. And operationalizing the framework will require the development of measures for each integrity dimension and for the maturity of each layer, a task this paper motivates and structures but does not complete.

IX. CONCLUSION

This paper has argued that the integrity of pharmaceutical distribution rests on two constructs that are routinely conflated or addressed in isolation. Traceability, the capacity to know what a unit is and where it has been, is necessary but not sufficient. Chain-of-custody integrity, the assurance that responsibility passed through an unbroken sequence of authorized custodians and that the unit and its condition were preserved, is the property that ultimately protects the patient, and it is frequently left implicit in standards, regulation, and research. The fragmentation of existing responses, each strong within its own track and silent about the others, produces systems that can be highly traceable yet weakly assured, advanced in identification and provenance while blind to diversion and condition failure.

In response, the paper has proposed an integrated conceptual framework. Four integrity dimensions, identity, provenance, custody continuity, and condition, define what integrity requires, and a five-layer architecture, spanning identification, event capture and exchange, custody verification, condition integrity, and governance, defines how it is produced. The integrative claim is that the lower layers deliver traceability while the upper layers convert that traceability into assurance, so that chain-of-custody integrity emerges only when the layers operate jointly within a governing institutional frame, supported by the cross-cutting enablers of interoperability, security, and trust anchoring. Applied to a stylized distribution system, the framework locates integrity gaps that traceability-centric approaches leave hidden, and it clarifies that the appropriate remedy for such a gap is the specific assurance layer the unaddressed dimension requires rather than more of the capability already in place.

Several directions for future research follow. The most pressing is empirical validation, including the development of measurement instruments for the four integrity dimensions and for the maturity of each layer, and the testing of the propositions across distribution systems that differ in structure and resourcing. Comparative studies of transaction-centric and end-point-centric regulatory models would sharpen understanding of the assurance gaps each leaves and of how they might be combined. Design-oriented research could examine how custody attestation and condition binding can be implemented on top of existing identification and event standards, and how lightweight versions can extend assurance to lower-resource settings without imposing unsustainable cost. And further work is needed on the governance arrangements and metrics that would make integrity, rather than mere visibility, the explicit objective of distribution system design. By naming chain-of-custody integrity as a distinct property and locating it within an integrated structure, the framework is intended to give regulators, supply chain actors, and technology designers a shared basis for that work.

REFERENCES

[1] Agbabiaka, J., Okonkwo, C. S., Ogunwole, O., Mayo, W., & Okeke, O. T. (2019). Supply chain risk management model for EPC and gas processing projects. Iconic Research and Engineering Journals, 3(2), 968-980. https://doi.org/10.64388/IREV3I2-1713124

[2] Akomolafe, O., & Agu, M. U. (2018). A conceptual model for enhancing internal audit quality through technology-enabled risk assessment frameworks. Iconic Research and Engineering Journals, 1(9), 458-475.

[3] Akomolafe, O., & Agu, M. U. (2019a). A conceptual framework for developing risk-based internal control models in the insurance and banking sectors. Iconic Research and Engineering Journals, 2(8), 335-354.

[4] Akomolafe, O., & Agu, M. U. (2019b). A review of data-driven risk evaluation models for emerging market financial institutions. Iconic Research and Engineering Journals, 3(6), 433-448.

[5] Akomolafe, O., & Agu, M. U. (2019c). Advances in financial resilience through integrated governance and compliance strategies. Iconic

Research and Engineering Journals, 2(10), 607-620.

[6] Aminu-Ibrahim, A. Y., Ogbete, J. C., & Ambali, K. B. (2018). Developing sustainable diagnostic laboratory infrastructure models for emerging and resource constrained health systems. Iconic Research and Engineering Journals, 1(8), 118-132. https://doi.org/10.64388/IREV1I8-1713586

[7] Aminu-Ibrahim, A. Y., Ogbete, J. C., & Ambali, K. B. (2019). Capital project delivery models for high risk healthcare infrastructure in developing national health systems. Iconic Research and Engineering Journals, 2(10), 626-649. https://doi.org/10.64388/IREV2I10-1713588

[8] Arumosoye, O. M., & Obriki, O. D. (2018). Development of an integrated heat stress risk conceptual model for industrial operations in extreme environments. Iconic Research and Engineering Journals, 1(12), 141-160. https://doi.org/10.64388/IREV1I12-1714415

[9] Arumosoye, O. M., & Obriki, O. D. (2019). Systematic review of near-miss and hazard observation data utilization in industrial safety management. Iconic Research and Engineering Journals, 3(2), 981-999. https://doi.org/10.64388/IREV3I2-1714417

[10] Blackstone, E. A., Fuhr, J. P., & Pociask, S. (2014). The health and economic effects of counterfeit drugs. American Health & Drug Benefits, 7(4), 216-224.

[11] Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017). Blockchains everywhere: A use-case of blockchains in the pharma supply chain. In 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM) (pp. 772-777). IEEE.

[12] Brechtelsbauer, E. D., Pennell, B., Durham, M., Hertig, J. B., & Weber, R. J. (2016). Review of the 2015 Drug Supply Chain Security Act. Hospital Pharmacy, 51(6), 493-500.

[13] Clauson, K. A., Breeden, E. A., Davidson, C., & Mackey, T. K. (2018). Leveraging blockchain technology to enhance supply chain management in healthcare: An exploration of challenges and opportunities in the health supply chain. Blockchain in Healthcare Today, 1.

[14] Commission Delegated Regulation (EU) 2016/161 of 2 October 2015 supplementing Directive 2001/83/EC of the European Parliament and of the Council by laying down detailed rules for the safety features appearing on the packaging of medicinal products for human use. (2016). Official Journal of the European Union, L 32, 1-27.

[15] Dagodzo, D. (2018a). A conceptual framework for UAV integration into national power grid inspection programs. Iconic Research and Engineering Journals, 2(5), 391-412. https://doi.org/10.64388/IREV2I5-1716082

[16] Dagodzo, D. (2018b). A review of UAV applications in electrical transmission line inspection: Methods, technologies, and challenges. Iconic Research and Engineering Journals, 2(6), 234-254. https://doi.org/10.64388/IREV2I6-1716083

[17] Dogbatsey, E. A., & Ebhojie, O. (2018). Budget compliance and statutory reporting in Sub-Saharan Africa: A systematic review of frameworks, gaps, and reform pathways. Zenodo. https://doi.org/10.5281/zenodo.20446859

[18] Dogbatsey, E. A., Ebhojie, O., & Oyeleye, A. O. (2019). Reconciliation control and financial workflow redesign in emerging market organizations: A conceptual framework. Zenodo. https://doi.org/10.5281/zenodo.20447103

[19] Dosunmu, A. A., & Ogundele, P. O. (2019). Security audit and enterprise risk assessment frameworks for resilient information systems. Iconic Research and Engineering Journals, 3(5), 434-447. https://doi.org/10.64388/IREV3I5-1713225

[20] European Parliament and Council. (2011). Directive 2011/62/EU amending Directive 2001/83/EC on the Community code relating to medicinal products for human use, as regards the prevention of the entry into the legal supply chain of falsified medicinal products. Official Journal of the European Union, L 174, 74-87.

[21] GS1. (2016). EPCIS standard (Version 1.2). GS1 AISBL.

[22] GS1. (2018). GS1 general specifications. GS1 AISBL.

[23] Institute of Medicine. (2013). Countering the problem of falsified and substandard drugs (G. J. Buckley & L. O. Gostin, Eds.). National Academies Press.

[24] International Organization for Standardization. (2007). Security management systems for the supply chain (ISO 28000:2007). ISO.

[25] Karlsen, K. M., Dreyer, B., Olsen, P., & Elvevoll, E. O. (2013). Literature review: Does a common theoretical framework to implement food traceability exist? Food Control, 32(2), 409-417.

[26] Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2018). Lessons learned from offline assessment of security-critical systems: The case of Microsoft Active Directory. Iconic Research and Engineering Journals, 2(6), 277-299. https://doi.org/10.64388/IREV2I6-1717205

[27] Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2019). Implementation of Active Directory for efficient management of enterprise networks. Iconic Research and Engineering Journals, 3(4), 608-627. https://doi.org/10.64388/IREV3I4-1717206

[28] Mackey, T. K., & Liang, B. A. (2011). The global counterfeit drug trade: Patient safety and public health risks. Journal of Pharmaceutical Sciences, 100(11), 4571-4579.

[29] Mackey, T. K., Liang, B. A., York, P., & Kubic, T. (2015). Counterfeit drug penetration into global legitimate medicine supply chains: A global assessment. The American Journal of Tropical Medicine and Hygiene, 92(6 Suppl), 59-67.

[30] Mackey, T. K., & Nayyar, G. (2017). A review of existing and emerging digital technologies to combat the global trade in fake medicines. Expert Opinion on Drug Safety, 16(5), 587-602.

[31] Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Oluoha, O. M. (2018). A conceptual framework for legal and ethical risk modeling in enterprise data protection governance systems. Iconic Research and Engineering Journals, 2(2), 207-226. https://doi.org/10.64388/IREV2I2-1714911

[32] Mbonu, I. S., Aliliele, C., Uzoka, E., & Oluoha, O. M. (2019a). A review of comparative data protection regulations and secure cloud implementation strategies across jurisdictions. Iconic Research and Engineering Journals, 2(9), 482-501. https://doi.org/10.64388/IREV2I9-1714912

[33] Mbonu, I. S., Iwuanyanwu, U., Uzoka, E., & Oluoha, O. M. (2019b). Advances in enterprise log analytics and automated incident response architectures using Python and SIEM platforms. Iconic Research and Engineering Journals, 3(2), 1000-1019. https://doi.org/10.64388/IREV3I2-1714915

[34] Moe, T. (1998). Perspectives on traceability in food manufacture. Trends in Food Science & Technology, 9(5), 211-214.

[35] Obogo, S. F., Ozobu, C. O., & Uduokhai, D. O. (2019a). Advances in leadership driven safety culture transformation in large construction workforces. Iconic Research and Engineering Journals, 3(5), 507-523. https://doi.org/10.64388/IREV3I5-1715497

[36] Obogo, S. F., Ozobu, C. O., & Uduokhai, D. O. (2019b). Development of a construction safety risk governance model for multi contractor high rise projects. Iconic Research and Engineering Journals, 2(9), 502-522. https://doi.org/10.64388/IREV2I9-1715495

[37] Obogo, S. F., Uduokhai, D. O., & Ozobu, C. O. (2019c). Systematic review of hazard identification and risk control practices in urban construction projects. Iconic Research and Engineering Journals, 2(12), 666-681. https://doi.org/10.64388/IREV2I12-1715496

[38] Obriki, O. D., & Arumosoye, O. M. (2018). Conceptual modeling of data-driven occupational safety risk control in large-scale energy infrastructure projects. Iconic Research and Engineering Journals, 1(7), 169-189. https://doi.org/10.64388/IREV1I7-1714414

[39] Obriki, O. D., & Arumosoye, O. M. (2019). A conceptual framework linking management safety walkthrough frequency and coverage to safety culture outcomes in mega projects. Iconic Research and Engineering Journals, 2(8), 355-374. https://doi.org/10.64388/IREV2I8-1714416

[40] Ogbete, J. C., Aminu-Ibrahim, A. Y., & Ambali, K. B. (2018). Optimizing laboratory spatial planning strategies to improve diagnostic accuracy, safety, and clinical throughput. Iconic Research and Engineering Journals, 2(1), 87-113. https://doi.org/10.64388/IREV1I7-1713587

[41] Ogbete, J. C., Aminu-Ibrahim, A. Y., & Ambali, K. B. (2019). Regulatory compliant design systems for molecular and pathology laboratories in highly controlled environments. Iconic Research and Engineering Journals, 3(4), 607-631. https://doi.org/10.64388/IREV3I4-1713589

[42] Okonkwo, C. S., Ogunwole, O., & Okeke, O. T. (2018a). Framework for strategic procurement optimization in oil and gas operations. Iconic Research and Engineering Journals, 1(7), 153-168. https://doi.org/10.64388/IREV1I7-1713119

[43] Okonkwo, C. S., Ogunwole, O., & Okeke, O. T. (2018b). Model for inventory availability and plant uptime improvement in energy facilities. Iconic Research and Engineering Journals, 2(4), 160-172. https://doi.org/10.64388/IREV2I4-1713120

[44] Okonkwo, C. S., Ogunwole, O., Okeke, O. T., & Mayo, W. (2019). Conceptual framework for cost reduction through contract negotiation and vendor governance. Iconic Research and Engineering Journals, 2(9), 468-482. https://doi.org/10.64388/IREV2I9-1713121

[45] Olsen, P., & Borit, M. (2013). How to define traceability. Trends in Food Science & Technology, 29(2), 142-150.

[46] Sunday, E. A., Omoegun, G. O., Essien, M. A., & Oluokun, O. A. (2019). Thermodynamic efficiency and control strategies in residential air conditioning systems. International Journal of Scientific Research in Civil Engineering, 3(3), 52-76.

[47] Toyoda, K., Mathiopoulos, P. T., Sasase, I., & Ohtsuki, T. (2017). A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. IEEE Access, 5, 17465-17477.

[48] U.S. Congress. (1987). Prescription Drug Marketing Act of 1987, Pub. L. No. 100-293, 102 Stat. 95.

[49] U.S. Congress. (2013). Drug Quality and Security Act, Pub. L. No. 113-54, 127 Stat. 587 (Title II, Drug Supply Chain Security Act).

[50] World Health Organization. (2010). WHO good distribution practices for pharmaceutical products (WHO Technical Report Series No. 957, Annex 5). World Health Organization.

[51] World Health Organization. (2011). Model guidance for the storage and transport of time- and temperature-sensitive pharmaceutical products (WHO Technical Report Series No. 961, Annex 9). World Health Organization.

[52] World Health Organization. (2017a). A study on the public health and socioeconomic impact of substandard and falsified medical products. World Health Organization.

[53] World Health Organization. (2017b). WHO global surveillance and monitoring system for substandard and falsified medical products. World Health Organization.