A Study to enhance Transparency in Physicians billings under Ontario Health Insurance Plan (OHIP) with Blockchain Technology

Research Project for Emerging Issues/Advanced Topics Course

Master of Forensic Accounting (MFAcc)

University of Toronto

Prepared by Jennifer Arun Mendes

May 31, 2021

For Prof. Leonard Brooks

ACKNOWLEDGMENTS

The author wishes to acknowledge suggestions made by my mentor, Mr. Narasimhan Elangovan, Chartered Accountant, India who is specialised in Systems Audit, Risk Management in Blockchain Technologies.

Table of Contents

List of Figures 6

List of Abbreviations 7

SUMMARY 9

INTRODUCTION 11

PART 1: Background 22

Healthcare in Ontario 22

Ministry of Health 22

Ontario Health Insurance Plan (OHIP) 26

Insured Physicians Services 28

Key Players in the Ontario Health care Sector 29

College of Physicians and Surgeons of Ontario (College) 29

The Ontario Medical Association (OMA) 29

Canadian Medical Protective Association (CMPA) 30

ADM or General Manager of OHIP 30

The Physician Payment Review Board (Board)(PPRB) 31

Primary Health Care 32

Primary healthcare Payment Models in Ontario 32

Compensation Schemes 32

The current OHIP infrastructure in Ontario Healthcare 35

Medical Claims Electronic Data Transfer (MC EDT) 35

Government of Ontario (GO) Secure 35

eHealth Portal' 36

Recent fraudulent OHIP physician billing practices 37

Lack of Oversight of Virtual Care Billing 41

PART 2: Evaluation of the OHIP physician billings and challenges 43
OHIP Billing Process 43
Examining the various laws of the OHIP billing review 45
Before 2005 45
Post Cory Report- Bill 171 (the Health System Improvements Act, 2006) 45
Bill 138 47
Evaluation of various legislations. 54
Challenges in the existing OHIP Physician billing & review system 56
PART 3: Problem statement & Research Methodology 59
Problem Statement 59
Research Methodology 59
Objectives of the Study 60
Scope of the Study 61
Limitations of the Study 61
PART 4: Literature Review 62
Section 1 of the Literature Review 63
The Fraud Triangle (FTT) & The Fraud Diamond Theory (FDT) 63
Fraud in healthcare 68
Provider Fraud & its types 69
Annual General Report 2016 73
News articles on the publishing of Physician billings 76
Section 2 of the Literature review 81
Manuals, Reference guides, Specifications 81
Blockchain 82
Smart Contracts 84

Standard features in all Blockchains 84
PART 5: Discussion.....86
Introduction 86
Results of the research interview..... 86
Suitability of Blockchain..... 88
Advantages of Blockchain Technology..... 90
Advantages of Smart Contracts 97
Blockchain advantages in the healthcare sector 102
Proposed Framework: Ontario Health Insurance Networks (OHIN)..... 106
Process with OHIN..... 108
Proposed Concept of OHIN..... 111
Proposed Architecture of OHIN 113
Proposed Online Appointment System..... 116
Proposed Smart Contract for OHIP physician claim processing..... 118
OHIN System Design using Blockchain 120
Privacy and security..... 123
Proposed Outcome of the Ontario Health Insurance Network 123
Role of a Forensic Accountant 128
Fraud prevention & detection 128
Proactive Approach 129
Fraud Risk Assessment..... 129
Limitations of Blockchain and Smart Contracts 131
Potential Limitations and Challenges of OHIN 134
Scope for future research..... 135
CONCLUSION.....136

Bibliography 138
Appendices.....150
Appendix 1: Technology Backbone for OHIN 150
Key Solution Design Principle 150
OHIN Solution Architecture..... 153
OHIN IT Strategy 157
OHIN Information Security Framework 158
Appendix 2: Bill 138, Schedule 15 162
Appendix 3: Interview Questions..... 163

List of Figures

Figure 1 Increase in the projected MOHLTC spending in 2019-2020 23
Figure 2 Total Ontario expenses projected in 2019-2020 24
Figure 3 MOHLTC projected spending in healthcare in 2019-2020 25
Figure 4 Ontario Health Ministry budget forecast for OHIP for 2019-20 26
Figure 5 Federal Support to Ontario 27
Figure 6 Current OHIP physician billing mechanism 43
Figure 7 Physician Post Payment Audit review process, applicable from May 1, 2021 .. 51
Figure 8 The Fraud Triangle 63
Figure 9 The Fraud Diamond 66
Figure 10 Types of fraud in healthcare 70
Figure 11 Advantages of Blockchain Technology 90
Figure 12 Advantages of Smart Contracts 97
Figure 13 Fraud: 10-80-10 Rule 106
Figure 14 Proposed Framework: Ontario Health Insurance Network (OHIN) 108
Figure 16 Online Appointment System under OHIN 116
Figure 17 Smart Contract working under OHIN 118
Figure 18 Proposed System Design under OHIN using Blockchain Technology 120
Figure 19 Limitations of Blockchain Technology and Smart Contracts 131
Figure 20 Key Solution Design Principles of OHIN using Blockchain technology 150
Figure 21 Proposed OHIN Solution Architecture 153
Figure 22 Proposed OHIN IT Strategy 157
Figure 23 Proposed OHIN Information Security Framework. 158

List of Abbreviations

API	Application Programming Interface
ADM	Assistant Deputy Minister
CIHI	Canadian Institute for Health Information
CMPA	Canadian Medical Protective Association
CLHIA	Canadian Life and Health Insurance Association
CPSO	College of Physicians and Surgeons of Ontario.
CFMA	Commitment to the Future of Medicare Act
CCM	Comprehensive Care Model
DoS	Denial-of-Service
DOJ	Departments of Justice
DLT	Distributed Ledger Technologies
EBS	Electronic Business Services
EMR	Electronic Medical Records
FHG	Family Health Group
FFS	Fee-for-Service
FDT	Fraud Diamond Theory
FTT	Fraud Triangle Theory
FWA	Fraud, Waste, and Abuse
FIPPA	Freedom of Information and Protection of Privacy Act
GM	General Manager of OHIP
GDP	Gross Domestic Product
HHS	Health and Human Services
HCV	Health Card Validation
HIA	Health Insurance Act
HSARB	Health Services Appeal and Review Board
IHFA	Independent Health Facilities Act
I&IT	Information and Information Technology
IPC	Information and Privacy Commissioner of Ontario
IBC	Insurance Bureau of Canada

IoT	Internet of Things
IFA	Investigative and Forensic Accountant
MCEDT	Medical Claims Electronic Data Transfer
MRC	Medical Review Committee
MLST	Medico-Legal Society of Toronto
MOH	Ministry of Health
MOHLTC	Ministry of Health and Long-Term Care
ODB	Ontario Drug Benefit.
OHIN	Ontario Health Insurance Network
OHIP	Ontario Health Insurance Plan
OHSIP	Ontario Health Services Insurance Plan
OLIS	Ontario Laboratories Information System
OMA	Ontario Medical Association
OMSIP	Ontario Medical Services Insurance Plan
OPP	Ontario Provincial Police
OWASP	Open Web Application Security Project
PCH	Patient Claim History
P2P	Peer-to-Peer
PHIPA	Personal Health Information Protection Act
PPRB	Physician Payment Review Board
PoA	Proof-of-Authority
PKI	Public Key Infrastructure
RPC	Remote-Procedure-Call
REST	Representational State Transfer
SSL	Secure Socket Layer
SOA	Service-Oriented Architecture
SC	Smart Contract
TSL	Transport Layer Security
US	United States.
VPN	Virtual Private Network

SUMMARY

Aim

This paper aims to better understand the current Ontario Health Insurance Plan (OHIP) physician billing process by laying out the processes associated with claims submitted by physicians under the OHIP in the current healthcare environment in Ontario and suggesting ways to improve transparency.

Background

The Ontario Health Insurance Plan (OHIP) is an inevitable part of every Ontario resident. There has been a public demand for increased transparency about the OHIP and how healthcare providers charge the province and, generally, the public for medically insured facilities. The Ontario government has responded by passing new legislation, making the photo health card mandatory, publishing physician-identified billings, and enhancing the audit process.

Methods

Multiple journal articles and newspapers are referred to for finding the present method of physician billing, claim process, and fraud.

Findings

The OHIP physician billings, which account for 25% of the Ontario Ministry of Health budget, lack transparency, impacting Ontario taxpayers.

Result

This paper proposes an Ontario Health Insurance Network (OHIN) framework using blockchain and smart contracts for a physician billing and claim process. The framework concentrates more on fraud deterrence than relying mainly on the audit process to improve transparency and guide the taxpayer's money to the best use.

Jennifer, excellent job providing an overview of your chosen project area. This provides a solid foundation from which to read your report.

INTRODUCTION

In Canada, everyone, regardless of their status, wealth, jobs, fitness, or age, has access to 'Universal health coverage.'[1]Since the Government funds the Universal Health Care System, the funding for this healthcare system is mainly aimed at improving public health. As a result, medical coverage is universal and unlimited regarding where medical care is obtained within Canada.

The healthcare system is administered at the provincial level. Section 11 of the Health Insurance Act (HIA) describes who is entitled to obtain OHIP coverage as a resident of Ontario. However, the healthcare system in Canada is not free. The publicly funded health care at the federal, provincial, and territorial levels is funded by the general revenue, such as personal taxes, corporate taxes, sales taxes, payroll levies, and other income.[2]

In 2019[3] , the Canadian Institute for Health Information (CIHI) estimated that Canada's total health care spending was forecast to hit $265.5[4] billion in that year or $7064 per person. Overall, health spending was expected to account for 11.5 percent of Canada's gross

[1]Canada | Commonwealth Fund. (n.d.). Retrieved from https://www.commonwealthfund.org/international-health-policy-center/countries/canada Accessed in April 2021

[2]Canada's Health Care System - Canada.ca. (n.d.). Retrieved from https://www.canada.ca/en/health-canada/services/health-care-system/reports-publications/health-care-system/canada.html Accessed in April 2021

[3] Published on Jan 28, 2021, 2021 release presents finalized 2018 actual health expenditures, updated 2019 preliminary estimates using current-year information.

[4] National Health Expenditure Trends | CIHI. (n.d.). Retrieved from https://www.cihi.ca/en/national-health-expenditure-trends Accessed in May 2021

domestic product (GDP).[5] Since 2014, real-term health spending per capita has increased by an average of 1.7 percent per year[6].

In this research paper, the data considered is for 2019 as the year 2020 is an exceptional year due to pandemics. The expenses associated with healthcare in the year 2020 do not follow the regular patterns.

Important distinction here. Very true that the pandemics data would not be representative of an average year. That said, it may also increase the urgency for greater transparency considering more fraud could be perpetrated during COVID times.

Healthcare fraud is estimated to be between 2 and 10%[7] in Canada, according to the Canadian Life and Health Insurance Association (CLHIA). The Canadian Institute for Health Information is projecting $265.5 billion in healthcare spending for the year 2019 that could translate into an exposure approximating upwards of $26.5 billion per year.

About two-thirds of Canadians have private insurance, which covers services not covered by universal health coverage. According to the Insurance Bureau of Canada (IBC)[8],

[5] Health spending | CIHI. (n.d.). Retrieved from https://www.cihi.ca/en/health-spending Accessed in April 2021

[6] National Health Expenditure Trends | CIHI. (n.d.). Retrieved from https://www.cihi.ca/en/national-health-expenditure-trends Accessed in May 2021

[7] Fighting Fraud, Waste and Abuse for a Healthy Business retrieved from https://www.claimsecure.com/en/whats-new-blog/2019/march/11/fighting-fraud-waste-and-abuse-for-a-healthy-business/ Accessed in April 2021

[8] As per IBC: We're fighting 'prolific fraud' in Canada | Insurance Business. (n.d.). Retrieved from https://www.insurancebusinessmag.com/ca/news/healthcare/ibc-were-fighting-prolific-fraud-in-canada-162456.aspx Accessed in May 2021

financial losses are far higher around the country, and the situation is only getting worse. Medical services fraud has been described as a top priority by the IBC, and various regulatory measures are being implemented to minimize the issue.

Henry Tso, the vice president of investigative services at the Insurance Bureau of Canada (IBC), states that prolific fraud has a burden that goes far beyond financial loss.

According to him, when criminals defraud the system, they incur actual human and financial costs. Everyone must pay. The insurance industry is not the only one who suffers; the Government, taxpayers, and emergency services are all affected. Every connection in the chain is harmed.

Healthcare fraud, waste, and abuse (FWA) is estimated to be 6.19 percent worldwide. Fraud and corruption remain a significant economic, legal, and policy issue in the US $3.5 trillion healthcare sector, with recoveries reported at the US $ 3 billion in the fiscal year 2019 alone by the Departments of Justice (DOJ) and Health and Human Services (HHS).[9]

There have been no high-profile cases of Canadian physician fraud on the magnitude of recent multibillion-dollar cases in the United States. Also, Medical fraud is not as aggressively prosecuted in Canada in comparison with the US. According to Scott James, a detective staff sergeant and unit commander of health fraud investigations at the OPP's

[9]Justice Department Recovers over $3 Billion from False Claims Act Cases in Fiscal Year 2019 | OPA | Department of Justice. (n.d.). Retrieved from https://www.justice.gov/opa/pr/justice-department-recovers-over-3-billion-false-claims-act-cases-fiscal-year-2019 Accessed in May 2021

Anti-Rackets Branch, things happening in the United States occur in Canada, Europe, and anywhere else. Nether it is quantified, nor is it tracked.[10]

However, as per Choosing Wisely Canada, up to 30% of Canada's tests, treatments, and procedures are potentially unnecessary.[11] [12] Unnecessary tests, treatments, and medical procedures provide no value to patients, may cause harm, necessitate additional testing to evaluate false positives, contribute to undue stress for patients and family members, and consume valuable time and resources. The main reason for overbilling is that that payment systems reward excess billing.

Kickbacks, misleading claims like billing for services not provided, upcoding and provisioning of medically inappropriate services, and unlawful self-referrals are examples of fraudulent health care. These types of fraud will have a significant detrimental effect on health care use because it wastes scarce resources and puts people at risk by treating them with needless care or denying them access to medically necessary treatments. It leads to an increased risk of not fulfilling the main aim of the universal healthcare system.

In Canada, family physicians serve as the gateway to the healthcare system, acting as gatekeepers to specialized services. In contrast, primary care services are designed to meet

[10]Miller, A. (2013). Medical fraud north of the 49th. In CMAJ: Canadian Medical Association journal = journal de l'Association medicale canadienne (Vol. 185, Issue 1). https://doi.org/10.1503/cmaj.109-4358

[11]Canadian Institute for Health Information. (2017). Unnecessary Care in Canada. Retrieved from www.cihi.cacopyright@cihi.caISBN978-1-77109-569-3 Accessed in April 2021

[12] Unnecessary Care in Canada: CIHI and CWC Joint Report Released - Choosing Wisely Canada. (n.d.). Retrieved from https://choosingwiselycanada.org/perspective/unnecessary-care-canada-cihi-cwc-joint-report-released/ Accessed in April 2021

most of the population's healthcare needs. These physician billings are one of the significant expenses in the Universal Healthcare System.

Ontario, the most populous province of Canada, also has one of the largest and complex publicly funded healthcare systems globally. Like other provinces, the physicians in Ontario do not bill individual patients. Still, they are remunerated through the Ontario Health Insurance Plan (OHIP) as per the schedule of fees as negotiated between the Ministry of Health (MOH) and the Ontario Medical Association (OMA). This arrangement is governed by the Health Insurance Act (HIA). Physicians are reimbursed through the fee-for-service model while others through the Alternate Payment Plans (APP). Physicians who belong to APP may also bill fee-for-service when providing services outside of the scope of these models. Primary care in Ontario has progressed from a fee-for-service (FFS) system of independent physicians to more advanced group-based practices based on patient enrolment and comprehensive care.

In 2018–2019, over 96 % of all physicians in Canada received a portion of their total payments through the Fee for Service (FFS) reimbursement model.[13] Likewise, in 2018-2019, 95% of General Practitioners in Ontario received fee-for-service payments from OHIP, but fewer than 30 % of them were paid solely on a fee-for-service basis.[14]

[13] *Summary report*. Physicians in Canada, 2019, Canadian Institute of Health Information, Page 33 Retrieved from https://secure.cihi.ca/free_products/physicians-in-Canada-report-en.pdf Accessed in April 2021

[14] Canada Health Act Annual Report 2019-2020, Retrieved from https://www.canada.ca/en/health-canada/services/publications/health-system-services/canada-health-act-annual-report-2019-2020.html Accessed in May 2021

Because of the nature of the Fee-for-Service Model, it is subject to a higher probability of fraudulent activities within the OHIP Physician billings. The need for transparency is evidenced by the auditor general's audit of the physician billing system in 2016, which included several recommendations to improve oversight.[15]In the December 2018 follow-up report, the Auditor General discovered that the ministry had not made significant progress on most of the recommendations. These included ascertaining physicians' operating costs, re-establishing inspectors to analyze physicians' records on-site, interviewing the physicians about the billings, and developing an effective mechanism to recover overpayments.[16] According to Bonnie Lysyk, Auditor General of Ontario, in 2018, the then-existing tool for recovering overpayments was ineffective, lengthy, and resource intensive.[17]

To combat healthcare fraud, the province of Ontario has implemented several fraud controls measures.

Ontario's Government switched to a secure photo health card for protecting the health care system from fraud. Red and white health cards are not accepted for Ontario Health Insurance Plan (OHIP) coverage as of July 1, 2020. The photo health card's advanced

[15] Office of the Auditor General of Ontario. (2016). Annual Report 2016. (Pages 551 to 603) https://www.auditor.on.ca/en/content/annualreports/arreports/en16/2016AR_v1_en_web.pdf Accessed in April 2021

[16] Oversight system for doctors' OHIP billings slammed as 'ineffective' - WWWHive. (n.d.). Retrieved from https://wwwhive.com/2019/07/01/oversight-system-for-doctors-ohip-billings-slammed-as-ineffective/ Accessed in April 2021

[17] Office of the Auditor General of Ontario. (n.d.). Retrieved from https://www.auditor.on.ca/en/content/annualreports/arreports/en18/v2_111en18.pdf Accessed in April 2021

security features help protect the public health system and are another way to get more value for the taxpayers' money.[18]

The province also has a toll-free fraud hotline and email address [19]for the public and healthcare providers to report any OHIP fraud to the ministry and send verification letters to select consumers to confirm the services. Correctly billed analyses its claim payment system regularly to detect patterns of activity that could indicate fraud and contracts with a special health fraud unit.

Furthermore, The Ministry of Health given data on 194 doctors who appeared in the Top 100 at least once between 2011-12 and 2017-18 fiscal years.

On December 10, 2019, Bill 138, the "Plan to Build Ontario Together Act," obtained Royal Assent. Bill 138's Schedule 15[20] amends the Ontario Health Insurance Act, bringing significant reforms to Ontario's provincial health insurance plan (OHIP). The auditing method for physician billings is one of the major reforms.

The OHIP General Manager, the Physician Payment Review Board (PPRB), the Health Services Appeal and Review Board (HSARB), and Bill 138: Amendments to the Independent Health Facilities Act and the Health Insurance Act are all well-known legal

[18] Government to phase out red and white OHIP cards | AFHTO. (n.d.). Retrieved from https://www.afhto.ca/news-events/news/government-phase-out-red-and-white-ohip-cards Accessed in May 2021

[19] OHIP Fraud - Ontario Health Insurance (OHIP) - Publications - Public Information - MOHLTC. (n.d.). Retrieved from https://www.health.gov.on.ca/en/public/publications/ohip/card_fraud.aspx Accessed in May 2021

[20] Plan to Build Ontario Together Act, 2019, S.O. 2019, c. 15 - Bill 138. (n.d.). Retrieved from https://www.ontario.ca/laws/statute/s19015#BK17 Accessed in May 2021

mechanisms aimed at disciplining the OHIP physician billing. The Amendment as per Bill 138 is annexed as Appendix 2.

While these regulatory mechanisms provide a solid deterrent to fraud and exploitation schemes, detecting and preventing them remains challenging.

Despite attempts to automate the identification of fraud by computational methods, including data analysis of OHIP payment claims data sets, the current system of relying on the stringent audit mechanism to identify fraud is beset with difficulties. As a result, innovative technologies are needed to improve the resilience, provenance, and verifiability of the OHIP claims that may be vulnerable to deception and misuse.

The topic of this research received impetus from the news article captioned 'Why can't patients see our OHIP billings? | The Star' in which Mr. David Musyj, president, and CEO of Windsor Regional Hospital, one of Ontario's most prominent hospitals outside of Toronto, contemplated OHIP billings. He opined that every Ontario resident should receive an annual statement[21] of the OHIP billings charged to their OHIP account or have online access to it. In his view, it will help resolve two issues, firstly to understand 'cost of services' and, in essence, to be individual auditors of those services.

Strong point here. Individuals would likely know immediately if something did not look right on their cost of services report.

[21] This was later through an email communication from Mr. David Musyj dated May 25, 2021, affirmed as 'in real-time'. Contacted by the researcher for the purpose of this research project.

In this research paper, reliance is placed on this concept. Hence, it is proposed to involve the patients as an essential part of OHIP claims by physicians to deter the possibility of fraudulent OHIP billings. The investigative and Forensic Accountant (IFA) role is widened to include evaluating processes and suggesting fraud prevention mechanisms using technology. In addition to the conventional part of uncovering information about financial irregularities, fraudulent activity, and commercial negligence by combining accounting, auditing, and investigative skills.

Good job integrating the IFA's role here.

The purpose of universal healthcare is to provide better healthcare to its residents, which is funded by the taxpayer's money. However, Governments have a responsibility to manage these funds effectively. Innovation and technology in the management of healthcare is needed to ensure the effective delivery of healthcare,

The Ontario Healthcare sector's core component is the Ontario Health Insurance Plan (OHIP), especially the Fee for service (FFS) reimbursement model for the physicians. This paper proposes a framework using technology to reduce inefficient and fraudulent practices in OHIP physician billing to improve transparency.

This research paper consists of five parts, which are listed below.

PART 1 of the research project covers the brief background of the Ontario Health Insurance Plan (OHIP), including the Ontario healthcare system, its key players, the primary care

model, and the existing infrastructure in the province. The background also includes recent cases from the news articles that depict fraud in OHIP billings and the most recent issue of Virtual Care Billing.

PART 2 discusses the current OHIP billing system and examines various OHIP-related legislation, including the time before and after the 2005 Cory Study, the 2016 Audit Report, and the introduction of Bill 138 in 2019. This section also covers the most recent Physician FFS Post-Payment Audit Process, which was implemented on May 1, 2021, as part of Bill 138. It emphasizes the challenges in the existing system and the need to improve transparency.

PART 3 contains the problem statement addressed in this research project and the Research Methodology, the Study's Objectives, the Scope of the Study, and the Study's Limitations.

PART 4 is a review of the literature. The Literature Review delves deeper into the Fraud Triangle and Fraud Diamond Theories and the importance of internal control, particularly in the healthcare sector. The literature review covers the types of fraud in healthcare, provider fraud in specific, and the categories of fraud in health care billing. This part comprehends the findings of the 2016 Annual Report, which reported practices in physician billings. The Toronto Star fought and won to get the highest OHIP billings published as part of the Transparency operation; various articles are covered in this regard.

The second section of the literature review comprises various references and manuals provided by the Ministry of Health about the OHIP. Furthermore, it included reviewing the latest technology, "Blockchain," and its application in "Smart Contracts." Blockchain has

common elements that make it suitable for most industries, including the healthcare industry.

PART 5 starts with the research focus area, Fee-for-service (FFS), understanding Blockchain technology's suitability because of the benefits of Blockchain Technology and Smart Contracts and their use in the healthcare sector. It further introduces the proposed framework (OHIN), which stands for Ontario Health Insurance Network. Two key processes, the Appointment System and Smart Contracts that enable automated payments to doctors are briefly summarized.

The existing OHIP billing and claim process is reviewed sceptically from the perspective of a Forensic Accountant. Accordingly, the OHIN framework concept is designed to find a solution for anti-fraud controls and improvised internal control.

This PART also discusses the potential, limitations, challenges of the proposed framework and future research scope.

PART 1: Background

Understanding the background of Healthcare in Ontario focuses on OHIP, its key players, infrastructure for OHIP physician billing, existing OHIP claim method.

Healthcare in Ontario

Canada is frequently referred to as a country with "socialized" medicine. However, its system differs significantly from countries where physicians are essentially state employees or where the entire medical profession is under centralized state control. In Canada, most medical practitioners work in private practice as consultants. Most doctors work out of their own offices, set their hours, and see patients who have chosen to visit them. The Government or an insurance plan does not assign doctors to Canadians.[22] The majority of Canadian provinces, including Ontario, operate similarly.

Ministry of Health

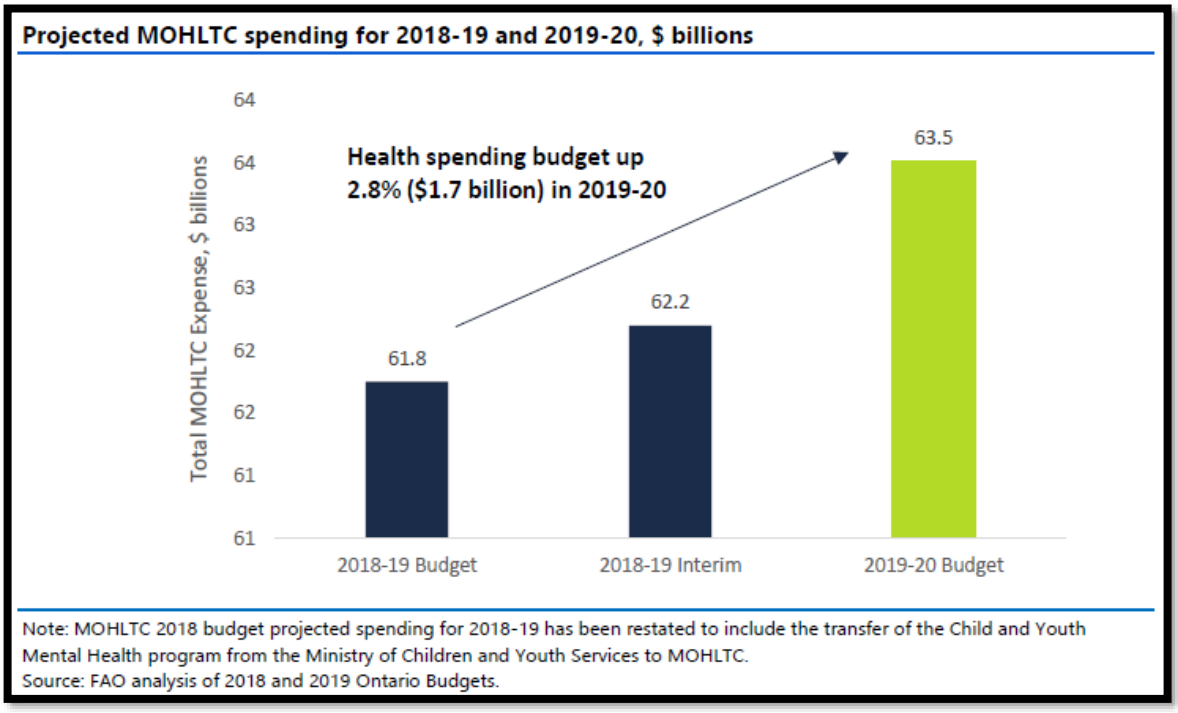
The Ministry of Health (MOH), earlier known as The Ministry of Health and Long-Term Care (MOHLTC)[23] , is the Government of Ontario ministry responsible for administering the healthcare system in Ontario[24].

[22] The Canadian Health Care System Retrieved from https://www.loc.gov/law/help/medical-malpractice-liability/canada.php Accessed in April 2021

[23] On June 20, 2019, the Ministry of Health and Long-Term Care was split into the Ministry of Health and the Ministry of Long-Term Care. Accessed in April 2021

[24] Ministry of Health (Ontario) - Wikipedia. (n.d.). Retrieved from https://en.wikipedia.org/wiki/Ministry_of_Health_(Ontario) Accessed in April 2021

Figure 1 Increase in the projected MOHLTC spending in 2019-2020

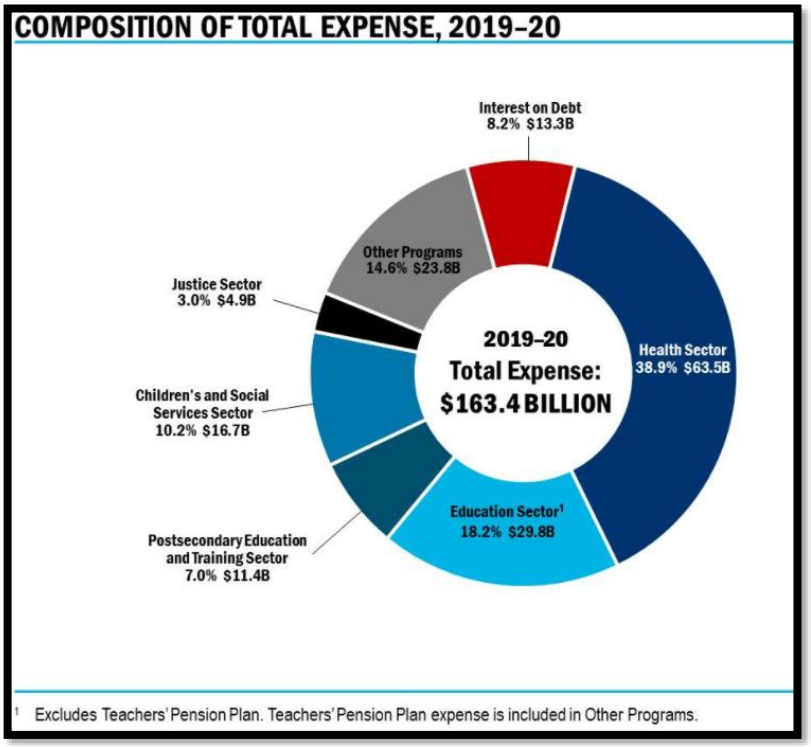


Source: FAO, Expenditure Estimates 2019-20

The Ministry of Health and Long-Term Care (MOHLTC) was expected to invest $63.5 billion in 2019-20, according to the 2019 Ontario Budget. The projected healthcare investment was a $1.7 billion (2.8%) boost over the health ministry's estimated investment in 2018-19, which was $61.8 billion in the 2018 budget.[25]

[25] Expenditure Estimates 2019-20: Ministry of Health and Long-Term Care. (n.d.). Retrieved from https://www.fao-on.org/en/Blog/Publications/estimates-health-2019 Accessed in April 2021

Figure 2 Total Ontario expenses projected in 2019-2020



Source: FAO, Expenditure Estimates 2019-20

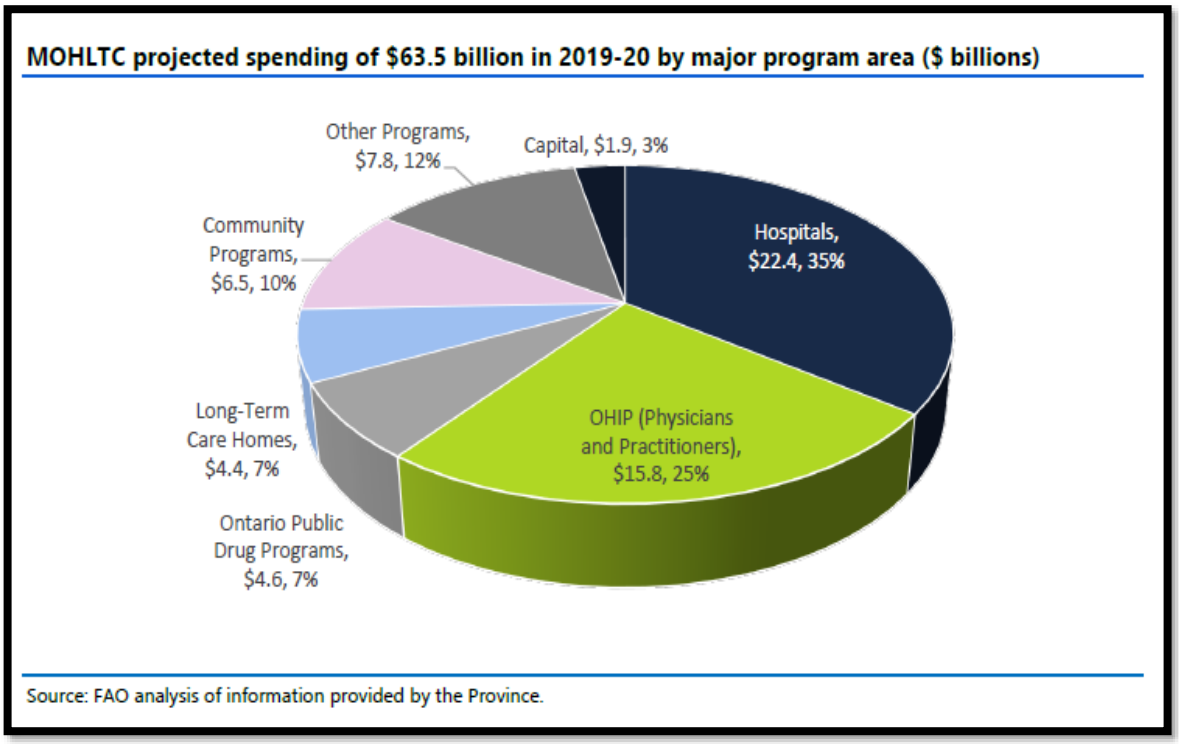
In 2019–20, this pie chart depicted the share of total Ontario expenditures by sector. In 2019–20, the total cost was $163.4 billion. The Health Sector is the most expensive, accounting for $63.5 billion or 38.9% of the total spending.

According to (Canadian Medical Association Masterfile, 2019), the Ontario province had 30,492[26] physicians in 2019. The allocated budget to OHIP (Physicians and Practitioners)

[26] Specialty CANADA NL PEI NS NB QC ON MB SK AB BC TERR Laboratory Medicine Specialists. (n.d.). Retrieved from https://www.cma.ca/sites/default/files/2019-11/2019-01-spec-prov_1.pdf Accessed in April 2021

was estimated to be $15.8 billion, which is 25% of the ministry budget of $63.5 billion and is roughly 9.7% of Ontario's $163.4 billion budget in 2019-20.[27]

Figure 3 MOHLTC projected spending in healthcare in 2019-2020



Source: FAO, Expenditure Estimates 2019-20

Sec. 2 of the Canada Health Act defines physician services as any medically required services rendered by medical practitioners.[28]

[27] 2019 Ontario Budget | Chapter 3. (n.d.). Retrieved from https://budget.ontario.ca/2019/chapter-3.html#t3-13 Accessed in April 2021

[28] Section 2 of the Canada Health Act. (n.d.). Retrieved from https://laws-lois.justice.gc.ca/eng/acts/c-6/fulltext.html Accessed in April 2021

Because OHIP expenditures account for more than a quarter of the Ministry of Health's budget, this study focuses on the transparency of OHIP physician billings and, as a result, increased accountability, and reduction of wasteful expenditure.

Ontario Health Insurance Plan (OHIP)

The Ontario Medical Services Insurance Plan (OMSIP) was established and enacted on July 1, 1966, and it was the province's first government-run health plan. The Ontario Health Services Insurance Plan (OHSIP) replaced it on October 1, 1969, as a provincially run cum federally assisted plan, under the federal 'Medical Care Insurance Act' to establish a national Medicare plan. In 1972, the plan's name was abbreviated to the Ontario Health Insurance Plan, or OHIP for short.

Figure 4 Ontario Health Ministry budget forecast for OHIP for 2019-20

Ontario health ministry spending by program area ($ billions)

	Actuals							Interim	Budget Forecast
Fiscal Year	2011-12	2012-13	2013-14	2014-15	2015-16	2016-17	2017-18	2018-19	2019-20
Hospitals	19.3	19.9	20.4	19.9	20.2	20.3	20.8	22.2	22.4
Growth		*3.3%*	*2.4%*	*-2.2%*	*1.4%*	*0.3%*	*2.8%*	*6.3%*	*1.3%*
OHIP	12.5	12.8	12.9	13.4	13.5	13.8	14.9	14.9	15.8
Growth		*2.3%*	*0.9%*	*3.5%*	*0.8%*	*2.3%*	*8.2%*	*-0.3%*	*6.2%*

Source: FAO analysis of data from MOHLTC, the 2019 Ontario Budget, and FAO.

Each Ontario resident with a primary and permanent residence in the province is entitled to emergency and preventive care under OHIP free of charge. Three sources fund OHIP are as follows:[29].

- The first source is payments transferred from the Government of Canada to fund health care partially. The Canada Health Transfer (CHT) is the most significant primary transfer to provinces and territories. In the year 2019-20, out of an estimated $63.5 billion, $15.6 billion was funded from CHT

Figure 5 Federal Support to Ontario

Federal Support to Ontario

In 2021-22, the Government of Ontario will receive $22.8 billion through major transfers.

Federal Support to Ontario
(millions of dollars)

	2012-13	2013-14	2014-15	2015-16	2016-17	2017-18	2018-19	2019-20	2020-21	2021-22
Major Transfers										
Canada Health Transfer	11,339	12,037	12,353	13,095	13,899	14,305	14,904	15,618	16,233	16,758
Canada Social Transfer	4,577	4,709	4,842	4,987	5,144	5,294	5,470	5,642	5,825	6,013
Equalization[1]	3,261	3,169	1,988	2,363	2,304	1,424	963	-	-	-
Total - Federal Support	**19,177**	**19,915**	**19,184**	**20,445**	**21,347**	**21,022**	**21,337**	**21,260**	**22,058**	**22,771**
Per Capita Allocation (dollars)	*1,431*	*1,471*	*1,404*	*1,483*	*1,530*	*1,496*	*1,493*	*1,464*	*1,497*	*1,523*

See additional notes
[1] Ontario does not qualify for an Equalization payment from 2019-20 onwards.

Source: Department of Finance Canada, Major federal transfers[30]

[29] Ontario Health Insurance Plan - Wikipedia. (n.d.). Retrieved from https://en.wikipedia.org/wiki/Ontario_Health_Insurance_Plan Accessed in April 2021

[30] Major federal transfers - Canada.ca Retrieved from https://www.canada.ca/en/department-finance/programs/federal-transfers/major-federal-transfers.html#Ontario Accessed in April 2021

- The second source is, by general, province tax revenues paid by the employer who is made to pay a payroll healthcare tax[31], which is financed by the payroll deduction tax paid by gainfully employed businesses and residents in Ontario.
- The third source is by premiums (taxes) paid by the residents of the province who pay a health premium[32]as part of their income taxes.

Though the patient does not have to pay when receiving the service, it is reaffirmed that Universal Health Care in Canada and Ontario is not without cost and is funded by various taxes and federal transfers.

Insured Physicians Services

Since Physicians and their OHIP billings are core to this research, regulation 552 of the HIA is referred to, which specifies insured physician services. A service which a physician provides in Ontario is an insured service under Regulation 552 of the HIA if it is:

- medically necessary.
- Referred to in Schedule of Benefits; and
- rendered in the circumstances or under the conditions specified in the Schedule of Benefits—Physician Services.

Physicians provide medical, surgical, diagnostic services and primary health care.

[31] with an exemption for small businesses
[32] introduced in 2004.

Key Players in the Ontario Health care Sector

College of Physicians and Surgeons of Ontario (College)

To protect and represent the public interest, the College oversees the practice of medicine in Ontario. It is empowered by the Regulated Health Professions Act, 1991, and the Medicine Act, 1991. It has the authority to self-regulate the medical profession in Ontario. Any physician who wishes to practice in Ontario must be a member of the College.

The Ontario Medical Association (OMA)

The OMA is a voluntary association to represent Ontario physicians' interests. It is recognized under the Health Insurance Act (HIA)[33] and Commitment to the Future of Medicare Act[34]. Through the OMA Representation Rights and Joint Negotiation and Dispute Resolution Agreement (OMA Representation Rights Agreement) dated December 2012, the Ministry recognizes the OMA as the exclusive bargaining agent of physicians.

Under the agreement, the Ministry and the OMA agreed to consult and negotiate in good faith to establish physician compensation[35] for physician services and related accountability in the publicly funded healthcare system. It generates the standardized Schedule of Benefits for Physician Services which describes the requirements for service reimbursement, applicable diagnostic and service codes, and their associated fees.

---

[33] Health Insurance Act, R.S.O. 1990, c. H.6. (n.d.). Retrieved from https://www.ontario.ca/laws/statute/90h06 Accessed in May 2021

[34] Commitment to the Future of Medicare Act, 2004, S.O. 2004, c. 5. (n.d.). Retrieved from https://www.ontario.ca/laws/statute/04c05 Accessed in April 2021

[35] MOHLTC - Resource Manual for Physicians - Section 2 - Physician Payment and Policy - 2.2. (n.d.). Retrieved from https://www.health.gov.on.ca/english/providers/pub/ohip/physmanual/pm_sec_2/2-2.html Accessed in May 2021

Canadian Medical Protective Association (CMPA) [36]

CMPA is a non-profit organization. In Ontario, every physician is required to obtain and maintain professional liability insurance. The Association receives membership dues and aids members who face medical-legal issues because they practice medicine. It also compensates people who have been affected by negligent medical treatment. Even though the physicians choose to use other liability-protection providers, nearly all Ontario physicians are members of this Association. Usually, the province reimbursed physicians around 87 % of their membership dues to the Association, which amounts to over $350 million.[37]

ADM or General Manager of OHIP

Section 4 of the Health Insurance Act enables the Lieutenant Governor in Council to appoint a General Manager for OHIP to administer the legislation[38]. Under section 4(2)(c), the General Manager has the authority to "make payments through the Plan for insured services, including determining eligibility and amounts."

Whether the General Manager believes that any or part of the covered service was not rendered or was misrepresented, or the service was not offered under agreed professional standards and procedure, the General Manager may pay a reduced amount or even refuse

[36] CMPA - About the CMPA. (n.d.). Retrieved from https://www.cmpa-acpm.ca/en/about Accessed in May 2021

[37] Office of the Auditor General of Ontario. (2016). Annual Report 2016. (Pages 551 to 603) https://www.auditor.on.ca/en/content/annualreports/arreports/en16/2016AR_v1_en_web.pdf Accessed in April 2021

[38] Health Insurance Act, R.S.O. 1990, c. H.6. (n.d.). Retrieved from https://www.ontario.ca/laws/statute/90h06#BK4 Accessed in April 2021

to pay for the service. This power is conferred by section 18(2) of the Health Insurance Act.[39] The General Manager can even refuse to pay or pay a reduced rate for services if, after consulting with a physician, the General Manager determines that any or all the services were not medically or therapeutically necessary.

The Physician Payment Review Board (Board)(PPRB)[40]

The Health Insurance Act created the Physician payment review board in 2010.[41] An independent adjudicative tribunal hears billing disputes between physicians and the Ministry when any party requests it. The PPRB is an independent adjudicative body that reviews disputes about payment between physicians and the General Manager (GM) of the Ontario Health Insurance Plan (OHIP) when a physician or the GM requests it.

After a hearing, the board can order the practitioner to refund the Ministry if it determines an overpayment, or the Ministry pays the physician if it determines an underpayment.

The revisions to the HIA and IHFA, among other reforms in Bill 138, overhauled the billing evaluation and review process for practitioner and hospital payments and moved the PPRB's duties to the Health Services Appeal and Review Board (HSARB)[42].

[39] Health Insurance Act, R.S.O. 1990, c. H.6. (n.d.). Retrieved from https://www.ontario.ca/laws/statute/90h06#BK4 Accessed in April 2021

[40] Primary Care Payment Models in Ontario - Health Care Professionals - MOHLTC. (n.d.). Retrieved from https://www.health.gov.on.ca/en/pro/programs/pcpm/ Accessed in April 2021

[41] Bulletin The Physician Payment Review Board becomes Functional. Retrieved from https://www.health.gov.on.ca/en/pro/programs/ohip/bulletins/4000/bul4511.pdf Accessed in May 2021

[42] Health Services Appeal And Review Board - Public Appointments Secretariat. (n.d.). Retrieved from https://www.pas.gov.on.ca/Home/Agency/294 Accessed in May 2021

Primary Health Care

Primary healthcare Payment Models in Ontario

Primary care, which covers illness prevention, health education, diagnosis, treatment, rehabilitation, and counselling, is the first point of interaction between a patient and the healthcare system. Primary care in Ontario has progressed from a fee-for-service (FFS) scheme of private physicians to more advanced group-based practices focusing on patient enrolment and comprehensive care.

In Ontario's Primary Care Renewal program, the Family Health Group (FHG) and Comprehensive Care Model (CCM) are payment models that pay in addition to the Fee for Service payment model. Both the FHG and CCM models provide a financial benefit to family physicians who provide quality health care to their patients and emphasize illness prevention. Both models encourage patients to enrol with their family physician to improve their connection with their physician and monitor their use of alternative health services outside of their family physician's care.

Compensation Schemes

Most physicians used to bill patients directly until Medicare was introduced in the late 1960s. Since the federal law was passed in 1966, the Ontario Health Insurance Plan (OHIP) was created, allowing patients to access medically required care in hospitals and physicians' clinics without paying upfront. Physicians started billing OHIP instead of issuing bills to patients or private insurers. Physicians have gone from being free to set their rates to negotiating schedules of fees with the government with the help of a representing body, OMA.

The physicians are paid out via the OHIP under three compensation streams.[43]

Fee for Service

Doctors were hesitant to become salaried employees when the Canadian provinces implemented universal healthcare. As a result, a fee-for-service system was developed. This payment model incentivizes physicians to focus on quantity rather than the quality of care.[44] Under fee-for-service, the physician's bill for each service they provide is a consultation, test, treatment, or procedure based on the OHIP's Schedule of Benefits. Though there are numerous codes, each physician will have a set of codes that best describe their service.

Patient Enrolment

Family physicians who work in group practices reimbursed a set amount for each patient signed up with them. Physicians form group practices (such as Family Health Organizations and Family Health Groups). They are compensated based on the number of patients registered and a predetermined basket of care provided to those patients. The aim is for family physicians to provide more systematic and consistent treatment to their patients. Bonuses, incentives, and other compensation for extra work, such as fee-for-service payments for programs not included in the basket of services, can be included in the remuneration. Family physicians could choose to enrol their patients in one of the patient-enrolment models or choose to practice on a fee-for-service basis.

---

[43] Primary Care Payment Models in Ontario - Health Care Professionals - MOHLTC. (n.d.). Retrieved from https://www.health.gov.on.ca/en/pro/programs/pcpm/ Accessed in April 2021

[44] Fee-for-service: an ethical conflict | Impact Ethics Retrieved from https://impactethics.ca/2017/02/22/fee-for-service-an-ethical-conflict/ Accessed in April 2021

Other-Payment contracts

These payment contracts are between the health ministry and specialist groups or workplaces such as hospitals and universities.

The majority of Ontario physicians' revenue comes from fee-for-service, which means they are paid for each service they offer according to the fees specified in the Schedule of Benefits.

The current OHIP infrastructure in Ontario Healthcare

In this research, an attempt is made to understand how the conventional method of the OHIP claims process works and the related infrastructure required by the physicians to submit these claims.

Medical Claims Electronic Data Transfer (MC EDT)

Medical Claims Electronic Data Transfer (MCEDT)[45] is a secure way of sharing electronic files between a registered MCEDT user and the Ministry of Health (MOH).

The MCEDT web service allows Electronic Medical Records (EMR) systems or integrated billing software to provide automated interfaces to initiate multiple concurrent uploads and downloads.

Government of Ontario (GO) Secure

The MCEDT method is exchanging actual claims, whereas the Government of Ontario (GO) Secure platform provides access to the submit service.

The eSubmit service provides a reliable electronic channel for sending documents to the ministry that contain personal health information. The documents include Remittance Advice Inquiries and the supporting documents needed to adjudicate complex cases, such as operative accounts, consult reports/notes, and so on.

[45] Ministry of Health and Long-Term care. (2018). Medical Claims Electronic Data Transfer (MC EDT) Reference Manual. https://www.health.gov.on.ca/en/pro/publications/ohip/docs/mc_edt_reference_manual.pdf Accessed in May 2021

eHealth Portal[46]'

The portal is a secure web-based viewer providing providers with a single point of access to their patients' digital health information, such as laboratory results, diagnostic images, and prescriptions for medication.

The information compiled under one portal helps healthcare providers give better healthcare advice and provide better care.[47]

[46] eHealth Ontario | It's Working For You. (n.d.). Retrieved from https://ehealthontario.on.ca/en/health-care-professionals/digital-health-services Accessed in May 2021

[47] eHealth Services (eHS) Info. (n.d.). Retrieved May 27, 2021, from https://www.ehealthontario.ca/wps/portal/eHealthPortal/Applications/EhsInfo/ Accessed in May 2021

Recent fraudulent OHIP physician billing practices

Doctors in Canada are highly qualified, having received extensive education and training as required by the Medical Council of Canada[48] , known worldwide for its high standards. The majority of doctors adhere to the highest ethical and professional standards, with few exceptions to this rule. Hence, there may also be double billing, overbilling, or even multiple billing due to either oversight or clinical staff error or fraudulent schemes. This research focuses on fraud prevention as well as the reduction of errors. The following are some of the dubious and fraudulent practices that have come to light.

Injection Mill[49]

A Star investigation revealed some physicians' unparalleled use of the controversial injections to treat chronic pain. It named one physician, Dr. Hany Demian, who billed OHIP for 1,999 nerve blocks to a single patient over three years[50], adding to the almost $8.4 million bills for the injections since 2014. Demian billed the province for more than 38,300 nerve block procedures in 2017/18 alone. In context, the governments of British Columbia and Saskatchewan claim that in the same year, all its physicians together performed only 55,000+ and 39,900+ respectively of the nerve block and epidural

[48] Medical Council of Canada. Retrieved from https://mcc.ca/ Accessed in May 2021

[49] 'That's an injection mill.' Ontario's top-billing pain doctors capitalize on province's lax rules, running up the public's tab for chronic pain management | The Star. (n.d.). Retrieved from https://www.thestar.com/news/investigations/2020/09/28/thats-an-injection-mill-ontarios-top-billing-pain-doctors-capitalize-on-provinces-lax-rules-running-up-the-publics-tab-for-chronic-pain-management.html Accessed in April 2021

[50] Ontario pain doctor billings 'shocking,' Doug Ford says after Star revelations | The Star. (n.d.). Retrieved from https://www.thestar.com/news/investigations/2020/09/28/ontario-pain-doctor-billings-shocking-doug-ford-says-after-star-revelations.html Accessed in April 2021

procedures. The tax-funded health system- OHIP has paid out more than $420 million for these kinds of injections since 2011.

Surgical Operation[51]

Dr. Andrew Taylor, who owned and operated Lasik Provision Niagara, a laser eye surgery clinic, was charged with fraud and forging documents in mid-2019. He was engaged in billing patients for surgical operations that were never done and instructing others on developing, changing, or otherwise modifying medical records relating to such procedures.

Misuse of Health Card[52]

In Ontario (College of Physicians and Surgeons of Ontario) v. Attallah, 2020[53], a physician was convicted of obtaining health card records from his patients' family members. He improperly billed OHIP with this detail and billed OHIP for interviews with relatives and services that he did not have. He was often accused of creating misleading or unreliable reports, such as medical charts, of justifying these billings.

[51] Niagara eye doctor charged with fraud | wellandtribune.ca. (n.d.). Retrieved from https://www.wellandtribune.ca/news/niagara-region/2019/07/11/niagara-eye-doctor-charged-with-fraud.html?rf Accessed in April 2021

[52] CPSO - Doctor Details. (n.d.). Retrieved from https://doctors.cpso.on.ca/DoctorDetails/Gabriel---Nicola-Attallah/0189886-77343 Accessed in April 2021

[53] Attallah (Re), [2020] OCPSD No 38, 2020 ONCPSD 38

***Surgeon in Whitby*[54]**

For three years ended in 2016, a 43-year-old Whitby surgeon has been charged with overbilling the health system by $170,000 over three years, according to the Ministry of Health.

***Billing in Ontario, while in India*[55]**

Dr. Ranjit Kumar Chandra, a medical physician, billed OHIP for over $2 million in fraudulent claims around 2012 and 2016. Due to ill health, he resided in India and had stopped practicing in Ontario. Dr..Chandra would pay patients for their OHIP numbers, and the patients would introduce family members and friends – to supply their OHIP card numbers and details for fake billings daily. He worked at six hospitals in Mississauga, Brampton, Etobicoke, and Scarborough and paid his medical assistants for their time.

***Medically impossible treatments*[56]**

The province's medical watchdog has charged one of Ontario's top-billing physicians with professional incompetence, alleging that he was negligent with his patient treatment and billed the Ontario Health Insurance Plan inappropriately.

---

[54] OPP charge Whitby doctor for fraudulent OHIP billings totalling $170K | CTV News. (n.d.). Retrieved from https://northernontario.ctvnews.ca/opp-charge-whitby-doctor-for-fraudulent-ohip-billings-totalling-170k-1.5176508 Accessed in April 2021

[55] Etobicoke doctor charged with defrauding OHIP: Longwoods.com. (n.d.). Retrieved from https://www.longwoods.com/newsdetail/8239 Accessed in May 2021

[56]One of Ontario's top-billing doctors faces discipline for alleged 'incompetent' care and inappropriate billings | The Star. (n.d.). Retrieved from https://www.thestar.com/news/investigations/2019/08/22/one-of-ontarios-top-billing-doctors-faces-discipline-for-alleged-incompetent-care-and-inappropriate-billings.html Accessed in May 2021

The claims against Christopher Anjema, a Chatham ophthalmologist who was the fourth largest biller in Ontario in 2017-18, are that he billed the province for conducting an unusual eyelid operation at a pace per patient that a specialist said was medically impossible. Dr. Christopher Anjema acknowledged that he did not uphold the profession's standard of practice in the treatment of his patients.[57]

Swap test 50 times more than average [58]

A doctor had his medical license revoked for "egregious deficiencies" in patient care and overbilling OHIP by more than $146,000. According to an audit, Gill billed for the swab test more frequently than any other family/general practitioner. While more than 90% of his peers coded it 500 times or less during the 2012-15 fiscal year, Gill claimed the fee code 25,000 times. One patient testified that she had never had the test in Gill's office, despite records indicating that he had billed OHIP for 11 of them in less than a year.

Excellent selection of examples here to highlight the nature of some of these fraudulent activities.

[57] "I AM ACCOUNTABLE": Chatham doctor who repaid OHIP $31Gs handed suspension | Toronto Sun. (n.d.). Retrieved from https://torontosun.com/news/provincial/i-am-accountable-chatham-doctor-who-repaid-ohip-31gs-handed-suspension Accessed in May 2021

[58] MANDEL: "Incompetent" Mississauga doc overbilled OHIP $146,000 | Toronto Sun. (n.d.). Retrieved from https://torontosun.com/news/local-news/mandel-incompetent-mississauga-doc-overbilled-ohip-146000 Accessed in May 2021

Lack of Oversight of Virtual Care Billing

The annual Value-for-money report[59] issued by Ontario Auditor General Bonnie Lysysk on December 7, 2020, further highlighted concerns about increasing the number of suspicious transactions in doctor billing. The report emphasized the province's lack of oversight of virtual care billings. According to the report, the Ministry has limited supervision over excessive virtual-care visits and billings. The Ministry has not made sufficient efforts to monitor and review questionable patterns of virtual-care usage via the Telemedicine Network and related physician billings.

Numerous instances were found where physicians had unusually high virtual-care billings and saw many patients in a single day. In 2019/20, a physician in a primary care practice, for example, had virtual-care billings of $1.7 million and saw as many as 321 patients virtually in a single day. In 2019/20, this physician also billed the Ministry for another $1.9 million in insured services (such as in-person care). A physician billed the Ministry $860,000 for nearly 17,500 virtual-care visits in 2019/20, but Telemedicine Network records revealed that this physician had fewer than 4,000 visits via the Telemedicine Network platform.

This is quite a staggering discrepancy. Really does show how some can perpetrate fraud during a pandemic.

[59] Value-for-Money Audit: Virtual Care: Use of Communication Technologies for Patient Care (2020). Retrieved from https://www.auditor.on.ca/en/content/annualreports/arreports/en20/20VFM_08virtualcare.pdf Accessed in May 2021

The Ministry is unaware of these discrepancies. It does not compare physician billing data with Telemedicine Network data to ensure that physicians use the Telemedicine Network appropriately for virtual-care billing.[60]

Although virtual care is not a substitute for traditional care in persons, the interest in virtual care has increased significantly due to public demand for comfort and timely access to health services. Hence it is vital to streamline to Billing process to avoid any fraudulent schemes, as stated in the above report.

Totally agree with you. The pandemic has changed the landscape of so many professions and made some a perfect breeding ground for fraudulent activities.

[60] Ibid

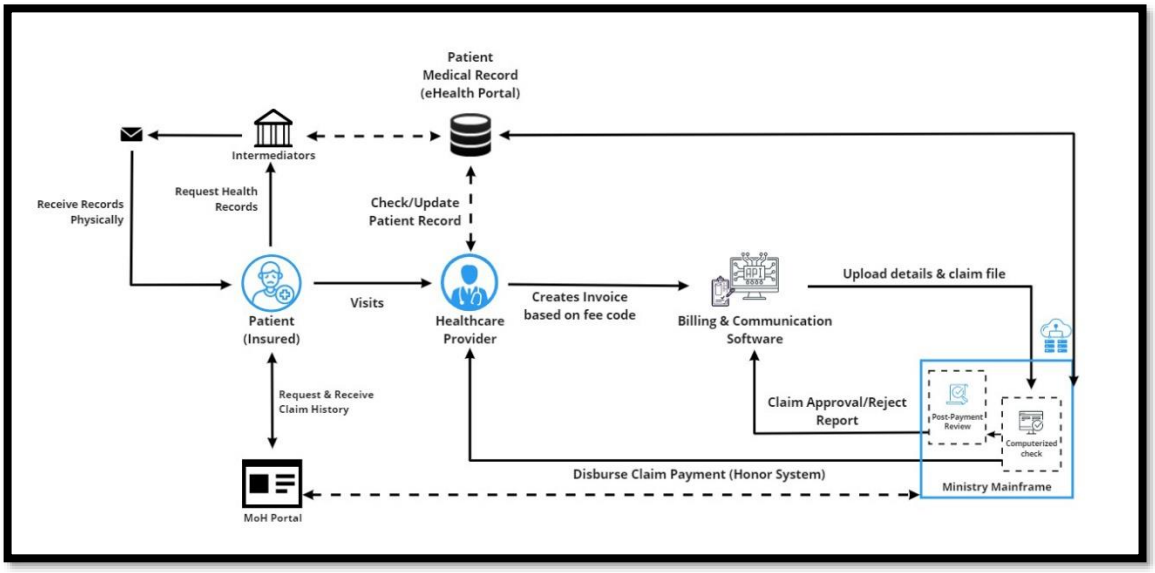
PART 2: Evaluation of the OHIP physician billings and challenges

OHIP Billing Process

The patient contacts the family physician's office directly to schedule an appointment or visits a walk-in clinic in the current system.

The current OHIP mechanism is represented as a block diagram,

Figure 6 Current OHIP physician billing mechanism



In periods of a pandemic or some other appropriate circumstance, the patient receives virtual care or generally attends the clinic in person. The physician prescribes medications or issues lab requisitions and treats the patients as required.

When a practitioner works under the fee-for-service model, he or she must make applications to OHIP to be reimbursed. Medical Claims Electronic Data Transfer (MCEDT) is the electronic data system used by OHIP to submit claims (MC EDT). It is a stable online system that lets physicians and third-party tech companies upload claims to

OHIP. MCEDT is the only method for submitting claims to the Ontario Ministry of Health. While physicians can manually file claims, most physicians choose to use an approved software system to upload claims and download reports more quickly and easily.

In essence, the practitioner submits 'invoices' to the Ministry of Health detailing who they met and what they did, and the Ministry of Health reimburses them for the health care services they rendered, which are covered under OHIP.

To be reimbursed by OHIP claim submissions, physicians must have the following details:

- the patient's information (to ensure they are registered for OHIP-insured services)
- a Fee Code and a Diagnostic Code from the 'Schedule of Benefits'

OHIP checks the claim and reimburses the physicians if it is approved. OHIP claim applications are processed monthly, around the 18th of each month. The "cut-off date" is the 18th of each month. All the claims made by that date will be assessed for payment by the 15th of the following month. When the 18th of the month arrives on a weekend or holiday, OHIP extends the deadline until the next working day.

Remittance Advice (RA) Report and a Claim Error Report are sent to the practitioners on the 5th and 7th of each month. These reports show which claims have been accepted, charged with adjustments, denied, or have any mistakes that will need correction before being paid. Physician billing for OHIP has remained consistent, and physicians are paid on an honour system. The process has evolved, emphasizing technology and mobile apps and extensive use of third-party billing providers. The OHIP billing audit and review mechanism, on the other hand, has evolved as new laws have been enacted.

Examining the various laws of the OHIP billing review

Under this part of the research paper, it is aimed to understand the legislations that surround the OHIP physician billings, audit, and review process

The operation mechanism of OHIP billing and claims and the understanding of the Schedule of Benefits on which doctors perform OHIP billing have undergone significant changes.

Before 2005

The Ontario Health Insurance Plan's billing audit process was administered by the Medical Review Committee (MRC), a College committee, but not a self-governing body. Billing with the Schedule of Benefits was seen as draconian because it was too restrictive; thus, Lyttle v OHIP in 2004 [61]was brought to court, and the court found that the scheme was inappropriate.

Post Cory Report- Bill 171 (the Health System Improvements Act, 2006)

Following the Cory Study, new Bill 171 was introduced, which established the Physician Payment Review Board, which oversaw whether medical services were appropriate and whether a physician is liable for false claims. It offered the Ministry of Health a variety of tools to obtain erroneous fees from doctors. In cases of outright fraud, the ministry could refer the matter to the Ontario Provincial Police's industrial crime unit. When a genuine controversy over billing code meanings occurs, the Physician Payment Review Board (PPRB) will hold a hearing.

[61] Lyttle v Ontario (Health Insurance Plan, General Manager), [2004] OJ No 4575, 134 ACWS (3d) 1103

OHIP Billing Review Process- Pre Bill 138

The Health Insurance Act (HIA), the Commitment to the Future of Medicare Act (CFMA), and the Independent Health Facilities Act (IHFA) give the Ministry the power to examine the physician's billing practices.

The Ministry of Health and Long-Term Care (the "Ministry") launched the "Payment Integrity Program" in the year 2006. The initial stage of the post-payment approval process for individual physician billings entails sending an educational letter to the physician outlining the reason for concern.

For evidence that the proper billing protocols were followed, specific patient records can be requested. Medical reports must show that an insured service was rendered to an insured individual, that the claim made accurately reflected the service rendered, and that the service was medically required.

Initially, claims are received and paid, and then the records check is used to verify what services were given and whether they equate to the fee claimed. Patients may receive confirmation letters to confirm that they received a particular service from a physician on a specific day.

A practitioner may also be obliged to reimburse the province for inappropriately submitted billings that were previously paid. The matter will be referred to the Physician Payment Review Board if the physician disagrees that a sum is owed or disagrees with the amount measured (PPRB).

Suppose a review of patient records or billing patterns reveals fraudulent billing behavior. In that case, the Ministry may refer the matter to the 'Accounting Policy and Financial

Reporting Branch,' which will investigate the possible fraud and, if necessary, refer the topic to the 'Ontario Provincial Police.'

The Ministry can also contact the College of Physicians and Surgeons of Ontario to investigate any alleged wrongdoing.

Bill 138[62]

The Ontario Medical Association (OMA) expressed reservations[63] about the new law and reintroduced a much tougher auditing scheme in the first version of Bill 138, which was passed in November 2019.

While physicians agreed that the OHIP billing system needed to be more transparent and accountable, however, there was strong opposition to a proposed auditing system that would give inspectors broad powers to dig into a physician's practice.

The Ministry made amendments to Bill 138 in response to OMA input and to work with the province's physicians.[64] Following Bill 138, several improvements to the OHIP billing mechanism were made under the HIA and the Commitment to the Future of Medicare Act. The revisions to the HIA and IHFA, among other reforms in Bill 138, overhauled the billing

[62] Ministry of Health, (2021). Summary of Physician FFS Post-Payment Audit Process Retrieved from https://www.health.gov.on.ca/en/pro/programs/ohip/docs/physician_FFS_post_pay_audit_process_summary.pdf Accessed in May 2021

[63] Proposed Changes to OHIP include Fundamentally Flawed Policies. (n.d.). Retrieved from https://www.newswire.ca/news-releases/proposed-changes-to-ohip-include-fundamentally-flawed-policies-815834078.html Accessed in April 2021

[64] Ontario Doctors Call for Changes to Proposed Audit System. (n.d.). Retrieved from https://www.newswire.ca/news-releases/ontario-doctors-call-for-changes-to-proposed-audit-system-895166275.html Accessed in April 2021

evaluation and review process for practitioner and hospital payments and moved the PPRB's duties to the Health Services Appeal and Review Board ("HSARB").

Before the changes, the Ministry has no authority to set off facility fees because of a billing disagreement or perceived overbilling. Furthermore, under the IHFA, there was no mechanism for an impartial investigation of billing issues for facility fees.

The Ministry is also expressly authorized to shape an opinion on facility fee overbilling, which creates an imminent debt that the Ministry will offset against the IHF's unpaid claims. It grants the licensee the freedom to get the billing case adjudicated by HSARB independently.

Despite the changes, Bill 138 contains reforms that would increase the intensity of audits and grant the General Manager of OHIP more power to deter, prosecute, and recover illegal payments to physicians. Physicians will be forced to have any documents requested by the General Manager, including personal information.

In addition, the review period for physician billings has been extended from 12 to 24 months[65]. Importantly, suppose there is any suspicion that the nature of the service was misrepresented or that the service was not medically required. In that case, the General Manager has the authority to refuse to pay a claim for payment for an insured service or to pay a reduced sum.

[65] Schedule 1 of the HIA enacted by Bill 138

Maintaining a record

Bill 138 establishes new record-keeping laws. According to these regulations, a licensee must keep all documents required to prove whether they rendered a service for which a facility fee was charged or paid, whether a service given was medically, therapeutically necessary, and that a service for which a claim was made was delivered.

The amendments state that if a claim for payment is not prepared in a specified way, the Minister has the authority to withhold payment for the service. New provisions further outline the specific scenarios in which the Minister can refuse to pay for services or pay reduced amounts, pay for services other than those described in a claim, or require reimbursement for amounts paid.

Billing Information Publication

Bill 138 creates a new power for the General Manager to disclose records relating to all payments made under the HIA to a specialist, practitioner, or health service, including patient information other than personal health information.

When the initial version of Bill 138 was issued, concerns were made on the potential adverse effects of this clause. It was proposed that contextual information surrounding the publication of physician billing information would be appropriate. The final version of Bill 138 clarifies that the General Manager cannot disclose the data obtained connected with the hearing.

However, the amended Bill 138 does address the main concerns with the new power as established under the said Bill.

Increased Fines and Liability

The IHFA amendments under Bill 138 broaden the circumstances in which the Director can revoke or suspend a physician's license.

The overall penalties for non-compliance with the requirements of the IHFA have at least doubled.

	Individual	Corporation
Pre - Bill 138 Amendments	First Offence: $25,000 Subsequent Offence: $50,000	First Offence: $50,000 Subsequent Offence: $200,000
Post - Bill 138 Amendments	First Offence: $50,000 Subsequent Offence: $100,000	First Offence: $100,000 Subsequent Offence: $500,000

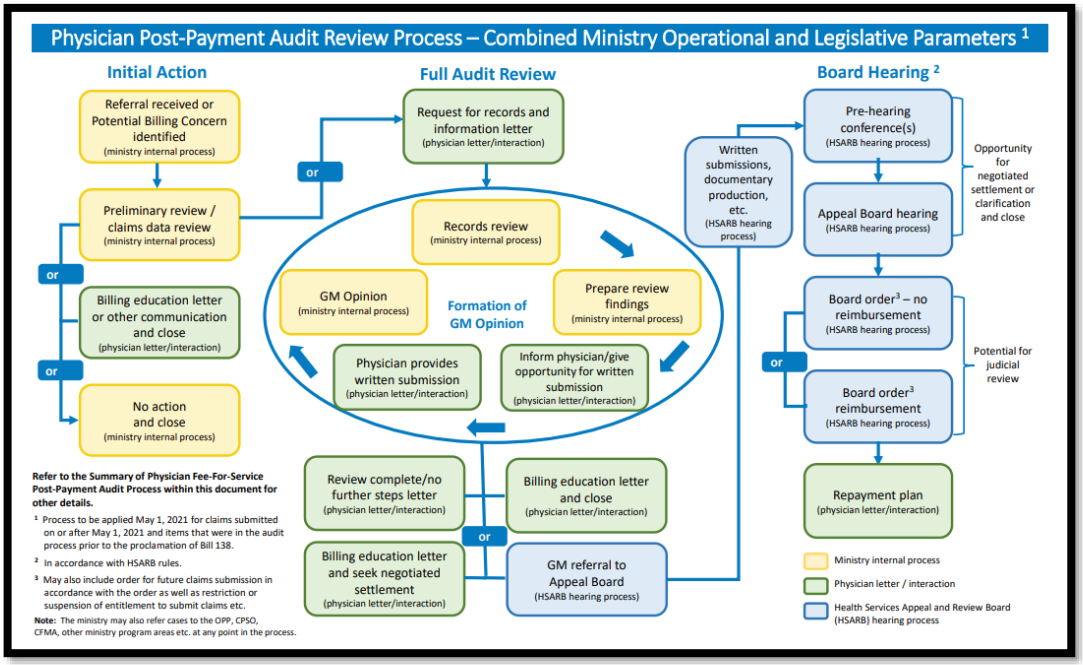
Physician FFS Post- Payment Audit & Review Process- Post Bill 138[66]

The Ministry of Health commits to provide information to help physicians submit appropriate claims. The Health Insurance Act (HIA) and Regulation 552 specify the OHIP payment conditions (including the Schedule of Benefits for Physician Services).

After being assessed by automated computerized checks that apply reimbursement conditions in compliance with the HIA, regulation 552, and the schedule of benefits, claims are paid on an 'honour' basis.

The following procedure will be followed for post-payment audits of physician billings.

Figure 7 Physician Post Payment Audit review process, applicable from May 1, 2021



Source: Ministry of Health website info bulletin[67]

[66] Ministry of Health, OHIP Division, (n.d.). The physician fee-for-service post-payment audit process. Retrieved from https://www.health.gov.on.ca/en/pro/programs/ohip/docs/physician_FFS_post_pay_audit_process.pdf Accessed in May 2021

[67] Ibid

The MOH will send a letter to the practitioner informing them of the investigation, including details on the audit process and requesting medical reports and other practice documents. The physician's details will help the ministry better identify the services rendered and decide if the fee schedule code(s) claimed are acceptable. Within two weeks, the MOH demands a letter from the physician confirming that the requested details will be sent to the ministry. In exceptional cases, the MOH can use an on-site reviewer to gather documents and other evidence at a physician's office. The Provider Audit Unit examines medical records to ensure that the fee plan code(s) billed are correct.

The Ministry is committed to ensuring that all payment conditions are met uniformly. Suppose the ministry is pleased with the physician's clarification of billing protocol and determines that the claims investigated were sufficient. In that case, the physician will be notified, and no further steps will be taken. The results of the ministry's audit will be defined in the General Manager's Opinion. The Ministry strives to complete audits as effectively and efficiently as possible while still supplying physicians with transparent, reliable, and timely information. The issue can be referred to the Health Services Appeal and Review Board (HSARB) by the General Manager (GM). The HSARB is a quasi-judicial adjudicative tribunal with the authority to resolve billing examination issues between the GM and physicians.

The entire audit process is completed in less than a year. If any side is dissatisfied with the Board's ruling, they can appeal to the Divisional Court of the Ontario Superior Court of Justice. The General Manager of OHIP (GM) oversees carrying out OHIP-related duties.

Combined Ministry Operational and Legislative Requirements for Physician Post-Payment Audit Review Process At any point during the procedure, the ministry can refer cases to the OPP, CPSO, CFMA, or other ministry program fields. For claims made on or after May 1, 2021, and products in the audit phase before the proclamation of Bill 138, the process will begin on May 1, 2021.[68]

[68] Ontario Health Insurance Plan INFO Bulletin. New Physician Post-Payment Review Process. (2021). https://www.health.gov.on.ca/en/pro/programs/ohip/bulletins/redux/bul210309.aspx Accessed in April 2021

Evaluation of various legislations.

Before 2005

The circumstance was so severe that Peter Cory, a retired Supreme Court of Canada judge, was called to investigate the powers of the Medical Review Committee (MRC). In his 2005 report, he discovered that Ontario's medical audit system had had a debilitating and, in some cases, devastating impact on physicians and their families. Because of this, there was a negative impact on the province's healthcare delivery. He further noted that the then prevailing medical audit system had harmed Ontario's appeal as a place to practice medicine, prompting some doctors to scale back their practices to stay within standard billing patterns. Hence there was a need for reform in the legislature, which was introduced under Bill 171.

Bill 171

However, The OHIP monitoring and control unit under the PPRB under the Bill 171 was blamed in 2016 by the Auditor General for failing to perform timely investigations of so-called anomalous billings. This paved way and return of more stringent audit policies in the OHIP billing and review process.

Bill 138

Post-payment examinations of physicians' claims for payment can be conducted under the jurisdiction of Section 18 of the HIA. Various principles govern the ministry's post-payment evaluation mechanism, which is structured to ensure procedural fairness, integrity, transparency, and accountability, as mandated by law. The audit procedure and

payment criteria are applied consistently and impartially, with review measures decided on a case-by-case basis.

These audits aim to detect possible billing issues, connect with physicians, and provide billing education. During this procedure, physicians have the right to request legal advice and be represented by legal counsel. The Ministry is dedicated to educating physicians on proper billing practices. When a possible billing issue occurs, the ministry's Provider Audit Unit analyzes the allegation. The bulk of billing issues are discovered because of tips or reports from the general population, healthcare staff, or other doctors.

The PPRB was abolished under Bill 138, adopted with the Fall Economic Statement of the year 2019. Two drastic measures as per Bill 138

Extrapolation, which the courts do not permit in other types of lawsuits unless robust expert evidence is given. If a bureaucrat believes a doctor billed wrongly in a sample of cases that he or she has collected, it is thought that the doctor billed incorrectly in all cases. The bureaucrat has the authority to order repayment in any situation, even though there is no evidence that it happened.

A return to the inspector style of inquiry, which has been seen to be time-consuming and costly. With the passage of Bill 138, the review mechanism, which serves as a detection tool, has become more stringent, potentially assisting in detecting fraud. The province and all of its physicians are likely to face challenges during the implementation of Bill 138.

The new legislation gives bureaucrats far more power to make decisions that affect all physicians rather than focusing on the few physicians who get involved in fraudulent schemes.

Challenges in the existing OHIP Physician billing & review system

There are specific challenges faced by healthcare providers and patients in the current OHIP physician billing and review system.

The tedious process of Patients' records, accessibility

When a patient requests treatment or services from a health provider, physician, pharmacy, or laboratory, their confidential information is usually recorded. The location of the treatment provided will usually maintain track, and the Ministry of Health will keep records of the facility billed to OHIP.

The Freedom of Information and Protection of Privacy Act (FIPPA)[69] of Ontario aims to safeguard private information kept by all provincial ministries and agencies. The Personal Health Information Protection Act (PHIPA)[70] regulates how personal health information is collected, used, and disclosed in the healthcare system. The Office of the Information and Privacy Commissioner of Ontario (IPC) oversees both Acts.

The patient has the right under the law to have all documents owned by the government kept private and has the right to see those documents as well. This right, however, does not always extend to non-governmental organizations.

[69] Freedom of Information and Protection of Privacy Manual: Chapter 1: The Legislation | Ontario.ca. (n.d.). Retrieved from https://www.ontario.ca/document/freedom-information-and-protection-privacy-manual/chapter-1-legislation Accessed in May 2021

[70] Ontario Ministry of Health and Long-Term Care - Health Care Providers - Declaration of PHIPA as substantially similar to PIPEDA - Q&A. (n.d.). Retrieved from https://www.health.gov.on.ca/english/providers/project/priv_legislation/phipa_pipeda_qa.html Accessed in May 2021

The Ministry of Health is generally in charge of keeping health records maintained by the Ontario government. Both include the patient contact history and the specifics of every OHIP-covered medical treatment the patient received, including blood tests, medical appointments, and hospitalization.

If the patient wishes to get this information, he can apply through the Ministry of Health portal, 'Patient claim history' (PCH)[71] , a computer record of claims paid by OHIP. Any individual has the right to access his personal health information under section 53 of the Personal Health Information Protection Act of 2004 (PHIPA). It keeps track of payments made to healthcare providers for services received under an individual's Ontario health card. It contains the details like the treatment dates, the healthcare worker who provided the services and the location of the services

A personal claims history is not a medical record but the history of the physician's treatments, which the physician has claimed under the OHIP. Furthermore, suppose the patient is interested in getting access to his electronic health record. In that case, he can gain access through 'eHealth Services[72]' to clinical applications such as Labs (OLIS), ODB Drugs, Diagnostic Images and Reports, and the Provider Directory. Because the digital health record comprises several different organizations, each must be contacted individually to retrieve the required information.

[71] Individual Personal Health Information (PHI) Access Requests - Ontario Health Insurance Plan - Ministry Programs - Public Information - MOHLTC. (n.d.). Retrieved from https://www.health.gov.on.ca/en/public/programs/ohip/phi_access/default.aspx Accessed in May 2021

[72] Accessing Your EHR | eHealth Ontario | It's Working For You. (n.d.). Retrieved from https://ehealthontario.on.ca/en/patients-and-families/accessing-your-ehr Accessed in May 2021

Extensive Reliance on Post Payment Audit Mechanism

The billing statements are subjected to a series of computerized reviews during the initial stage of the OHIP physician claim submission process. However, the Payment Integrity Program's first stage works on an "honour scheme," with automatic checks that are not rigorous, and claims processed as submitted to ensure timely payment. Following payment of OHIP billing claims, they are checked on a post-payment basis.

Individual reviews may be triggered by publicly communicated or internally recorded issues at the OHIP processing office. In addition, the Ministry will study OHIP accounting procedures and identified payment problems throughout the province.

Improper billing activities that come under the Ministry's investigational jurisdiction can vary from basic errors like wrongly noting the type of care given to falsely claiming a higher fee code to even fraudulently overbilling for insured services. The Ministry will also investigate charges for access to insured facilities that violate the CFMA.

Due to the lack of patient involvement, fraud in OHIP claims is a likelihood.

Traditional health care claims authentication and payment entail the health care provider submitting a claim after providing treatment to a patient, which the payer then verifies and reimburses. However, in this entire OHIP claim process, a vital stakeholder is left out of this process: the patient for whom the service is provided. The patient is unaware of the services billed and the time, date, and place of service in the claim submitted by the practitioner, which provides an opportunity for fraudulent schemes.

PART 3: Problem statement & Research Methodology

Problem Statement

The OHIP physician billings account for 25% of the Ontario Ministry of Health budget, which lacks transparency, impacting Healthcare, Government, and Ontario taxpayers.

Research Methodology

In this research paper, the literature review is performed in two areas. First, to review the literature on the OHIP billing frauds and secondly, on the Blockchain technology.

University of Toronto Library, Google Scholar, newspapers, Ministry of health website are used to search for articles, journals, and manuals.

In this review, the following procedure is used to get the relevant literature.

- Made a list of keywords and searched in the title of the article *(Keywords: Healthcare, Transparency, Fraud, Fraud schemes, Healthcare frauds, Global Healthcare, Blockchain, Smart contracts, OHIP, Ontario Health insurance plan, electronic health records, electronic medical record*)
- Fine-tune keywords depending on the set of results.
- It was sorted the findings by title, excluding non-supported languages and documents that are explicitly unrelated.
- Read the abstracts to narrow down the findings.
- Identified the concepts by reading the articles that follow in greater depth.

The results provide a diverse set of articles, most of which had healthcare fraud but no direct linkage to OHIP claim. The series of articles went through a rough screening process, with relevance determined by the work's title and abstract. Blockchain and Smart Contracts' advantages were reviewed from various industries as the common elements apply to all sectors, including Healthcare.

This research topic gained momentum from a thought expressed by Mr. David Musyj, the President and CEO at Windsor Regional Hospital (WRH)[73], Ontario, Canada. During this research, Mr. Musyj was approached to get insight from him as a healthcare industry expert. He was requested to provide his opinions on three questions as mentioned in Appendix 3.

Objectives of the Study

1. To understand the current Ontario Health Insurance Plan (OHIP) claim method by outlining the processes associated with claims submitted by the physician under the OHIP within the current healthcare environment in Ontario.
2. To evaluate the Ontario Health Insurance Plan (OHIP) claim method and derive scope for improved transparency.
3. To propose a framework for Ontario Health Insurance Network (OHIN) to facilitate the transparency in the physicians' OHIP billings.

[73] Windsor Regional Hospital is Ontario's 15th largest hospital and its 7th largest community teaching hospital, serving approximately 400,000 people in Windsor and Essex County.

Scope of the Study

With the increase in the amount spent on healthcare in Ontario, there has been an increasing demand for transparency in the OHIP physician claims, which is the significant component of the healthcare expenditure in Ontario. Given this situation, the present study analyses the scope for increasing transparency in the OHIP physician billings. The area of the study is restricted to the province of Ontario, Canada. The research focuses on the transparency in the physicians billing on OHIP for the Fee-for-Service (FFS) reimbursement model for the services rendered to the patients. This study was conducted in April and May month of 2021.

Limitations of the Study

The province pays for many health services for patients with a valid Ontario health card through OHIP, Ontario's health insurance plan. Appointments with family physicians, visits to walk-in clinics, visits to emergency rooms, medical tests, and surgeries are among the many services available.

However, only health services as provided by a family physician are discussed in this research paper. This study is also limited to family physicians paid on a fee-for-service basis, accounting for a significant portion of all general practitioners.

PART 4: Literature Review

Since the research topic involved fraudulent OHIP claims, Section 1 of the literature review evaluates the two theories: The Fraud Triangle Theory (FTT) and the Fraud Diamond Theory (FDT). After assessing the core components required for committing fraud as per these theories, the literature review extended to understand the prevailing types of fraud in the healthcare sector. The Annual report of 2016 from the Auditor General of Ontario was analyzed to comprehend the observations in the Physician's billings and the recommendations.

The transparency in the OHIP physician billing has been a long-discussed issue. A 2014 Freedom of Information request was filed by health reporter, Theresa Boyle which launched the fight to get the highest OHIP billings. Various news articles were published over five years, and they are an essential part of the literature review for this study.

The purpose of Section 2 of the literature review was to learn about the current OHIP physician billing method. This review covered the various manuals, technical specifications, and physician reference guides provided by the Ministry of Health for the current system's operation.

Furthermore, understanding Blockchain technology and Smart Contracts as part of the literature review. The focus of the literature review was on the benefits and challenges of Blockchain technology and Smart Contracts across all industries and the common thread that makes it appealing to the healthcare industry. In addition, the use cases of Blockchain technology were examined for comprehending the challenges.

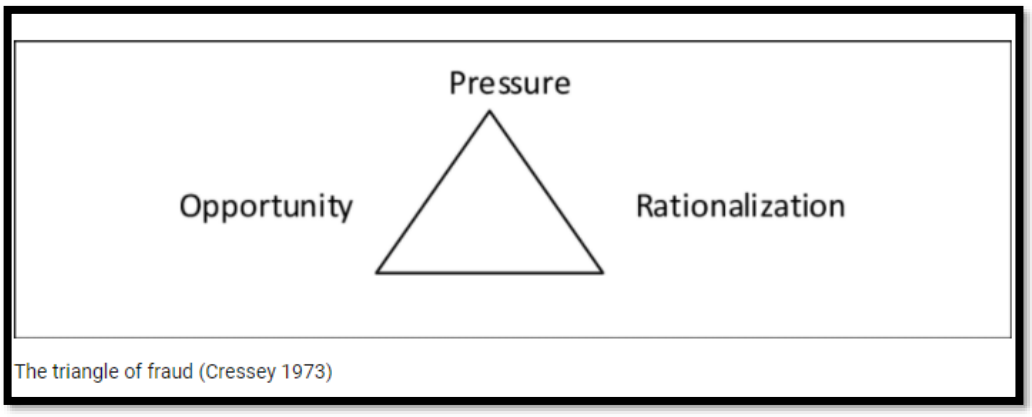
Section 1 of the Literature Review

The Fraud Triangle (FTT) & The Fraud Diamond Theory (FDT)

According to Donald Cressey, a criminologist who pioneered fraud by arguing that everything people do must have a reason. There must be a reason for everything they do. Cressey defines the three factors as pressure, opportunity, and rationalization, all of which must be present for fraud to occur.

The second requisite factor for fraud to occur is the perceived opportunity, the core focus area in this research paper.

Figure 8 The Fraud Triangle



Source: (Thornton et al., 2015)

Internal control weaknesses create an opportunity for a person to commit corporate fraud. According to the principle of perceived opportunity, people can take advantage of available situations.

An ineffective control or governance system creates an opportunity for an individual to commit fraud.[74] According to the concept of perceived opportunity, people will take advantage of available circumstances.[75] In most cases, according to Cressy, the lower the risk of fraud is discovered, the more likely it will occur. Opportunity[76]is the ability to circumvent fraud controls.

Furthermore, financial fraud cannot occur unless an opportunity exists.[77] The inherent susceptibility of the company's accounting to manipulation and the conditions within the company that may allow fraud to happen are two aspects of the opportunity.

Lack of monitoring and supervision (oversight), weak internal controls, a lack of an audit trail, and irregular job rotation contributes to the fraudster's belief in opportunity.[78]

Similarly, in the context of OHIP claim processing, emphasis can be placed on reducing the opportunity by strengthening the internal controls by involving the patient as an

[74] Mansor, N., & Abdullahi, R.' U. (2015). Understanding the Convergent and Divergent for Future Research Article in International Journal of Academic Research in Accounting Finance and Management Sciences · October. https://doi.org/10.6007/IJARAFMS/v5-i4/1823 Accessed in April 2021

[75] Kelly, P., & Hartley, C. A. (2010). Casino gambling and workplace fraud: a cautionary tale for managers. Management Research Review, 33(3), 224–239. https://doi.org/10.1108/01409171011030381 Accessed in May 2021

[76] Wilson, A. (2004). Employee Dishonesty: National Survey of Risk Managers on Crime. In Journal of Economic Crime Management Winter (Vol. 2, Issue 1.https://www.utica.edu/academic/institutes/ecii/publications/articles/BA2D546B-BC9E-1844-8B0ADF5FB1B84B99.pdf Accessed in April 2021

[77] Fraud risk formulas for financial statement audits. (n.d.). Retrieved from https://www.researchgate.net/publication/228804816_Fraud_risk_formulas_for_financial_statement_audits Accessed in April 2021

[78] Kenyon, W. and Tilton, P. D. (2006). Potential Red Flags and Fraud Detection Techniques - A Guide to Forensic Accounting Investigation - Wiley Online Library. (n.d.). Retrieved from https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119200048.ch13 Accessed in May 2021

essential component to validate the claim process. Suppose the claim submission process is designed to be robust. In that case, the risk of any fraudulent billing being discovered will likely deter any health care provider from engaging in the fraudulent schemes or any erroneous billings.

Valid point here and good integration of course concepts.

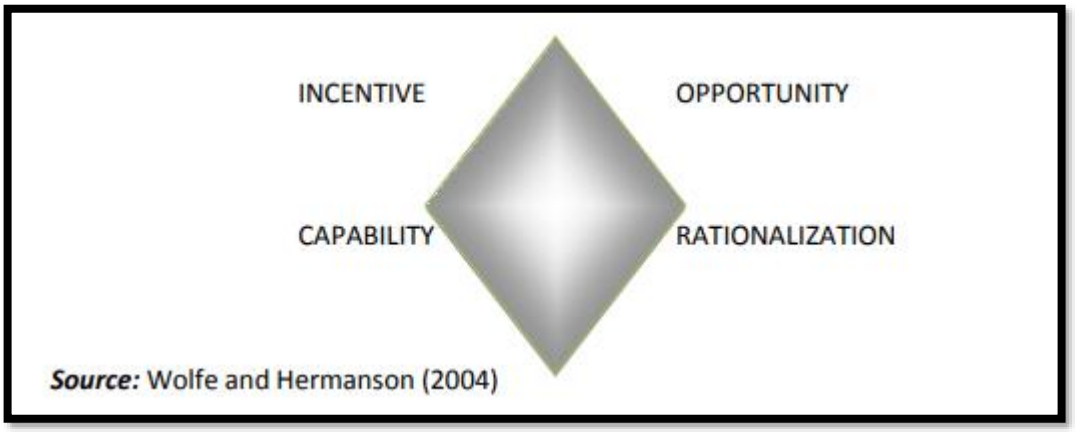
As stated above, increased oversight from the patients in the validation process of the claim will further dissuade the health care provider.

Wolfe and Hermanson first published the FDT in the CPA Journal in December 2004. In this principle, a capability dimension has been introduced to the Fraud Triangle Theory (FTT's) three original fraud elements. While perceived pressure may coexist with an incentive and a rationalization, fraud is unlikely to occur unless the fourth factor (i.e., capability) is also present.[79] The prospective fraudster must possess the necessary expertise and abilities to commit fraud.

According to Wolfe and Hermanson, an opportunity opens the door to fraud, while motivation (i.e., pressure) and rationalization lead a person to the door. On the other hand, Capability enables a person to see the opportunity through the open doorway and take advantage of that by walking through it regularly.

[79] Wolfe, D. T., & Hermanson, D. R. (2004). The Fraud Diamond: Considering the Four Elements of Fraud. https://digitalcommons.kennesaw.edu/facpubs Accessed in April 2021

Figure 9 The Fraud Diamond



Fraud increases the overall costs for vital health care services and can potentially be harmful to Medicare and Medicaid beneficiaries[80]

The four components of the Fraud Diamond theory can be categorized into two categories:

No Control- Rationalisation, Incentive/ Pressure

Rationalization

Rationalization is the existence or appearance of attitudes, characters, or a collection of ethical principles that permit management or workers to commit unethical acts. Rationalization is the process of justifying a course of action. Cheating actors would always seek logical explanations for their behavior, and this cannot be controlled.

[80] Recommendations to protect patients and health care practices from Medicare and Medicaid fraud. (n.d.). Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7323645/

Pressure

Pressure is the need to commit and conceal the crime. The pressure will come from an urgent need to address a problem (financial pressure), which cannot be shared. The issue will be closed by the individual involved, and it will no longer be shareable. This component of the Fraud Diamond cannot be controlled.

Possibility of Control- Opportunity & Capability

Opportunity

An individual may commit fraud if there is a lack of control. Since the suspect assumes that their actions would not be noticed, chances are created. Until the activity is identified, no severe measures shall be taken to respond to it. Opportunities are generally attributed to a lack of internal controls and oversight.

*Capability (*competence / abilities)

In this situation, competence refers to someone's ability to commit fraud. As a result, competence can be described as an employee's ability to breach company internal controls, create sophisticated embezzlement tactics, and manage a social situation favoring him by influencing others to work.

With proper internal controls in place, streamlined claim mechanism, power can be exercised on the Opportunity and the Capability Components of the FDT.

Fraud in healthcare

The insurance industry is vulnerable to fraud. Healthcare fraud is one of the standard types of insurance fraud. Health care fraud is defined as an intentional act of defrauding a health care benefit program or obtaining money or other property owned by a health care benefit program through false representations.

Health care fraud schemes can be among the most complex due to the highly technical nature of this industry. It is necessary to understand and investigate the healthcare & payment system type to comprehend and analyze a healthcare fraud scheme.

There are two types of healthcare systems, one that the private parties pay and the other that is funded by Government programs. The differences in each system have the most significant impact on who is defrauded. Government programs in countries with universal health care, such as Canada, can be particularly vulnerable to healthcare fraud. Payment systems are concerned with how money is transferred from those who pay for services to those who provide them.

Direct payment, single-payer, and third-party payer are the three most common payment systems, and each can exist in the same country. The Single-Payer system is used in Ontario, Canada.

In a single-payer system, such as the one used in Ontario, Canada, a government healthcare program pays the healthcare providers on behalf of the patients who receive services. In other words, the government is the "single-payer," and it delegated most of the service delivery responsibilities to private healthcare providers.

Provider Fraud & its types

Provider fraud refers to practices by healthcare providers (such as practitioners, medical suppliers, and medical institutions) that result in unnecessary costs to healthcare programs or patients by reimbursing for unnecessary or excessive services or services that do not meet recognized healthcare standards.

For several reasons, provider fraud is a particularly pervasive risk in the healthcare industry. Providers have the necessary knowledge of medical techniques, procedures, and terminology to avoid being questioned by claim-handling personnel.

Furthermore, government healthcare programs contract directly with the healthcare providers for billing arrangements, leaving patients uninformed and uninvolved. Patients are also hesitant to accuse physicians of wrongdoing because they rely on the provider's ongoing services. Also, when providers engage in fraudulent practices, they frequently forgive any out-of-pocket expenses incurred by the patient.

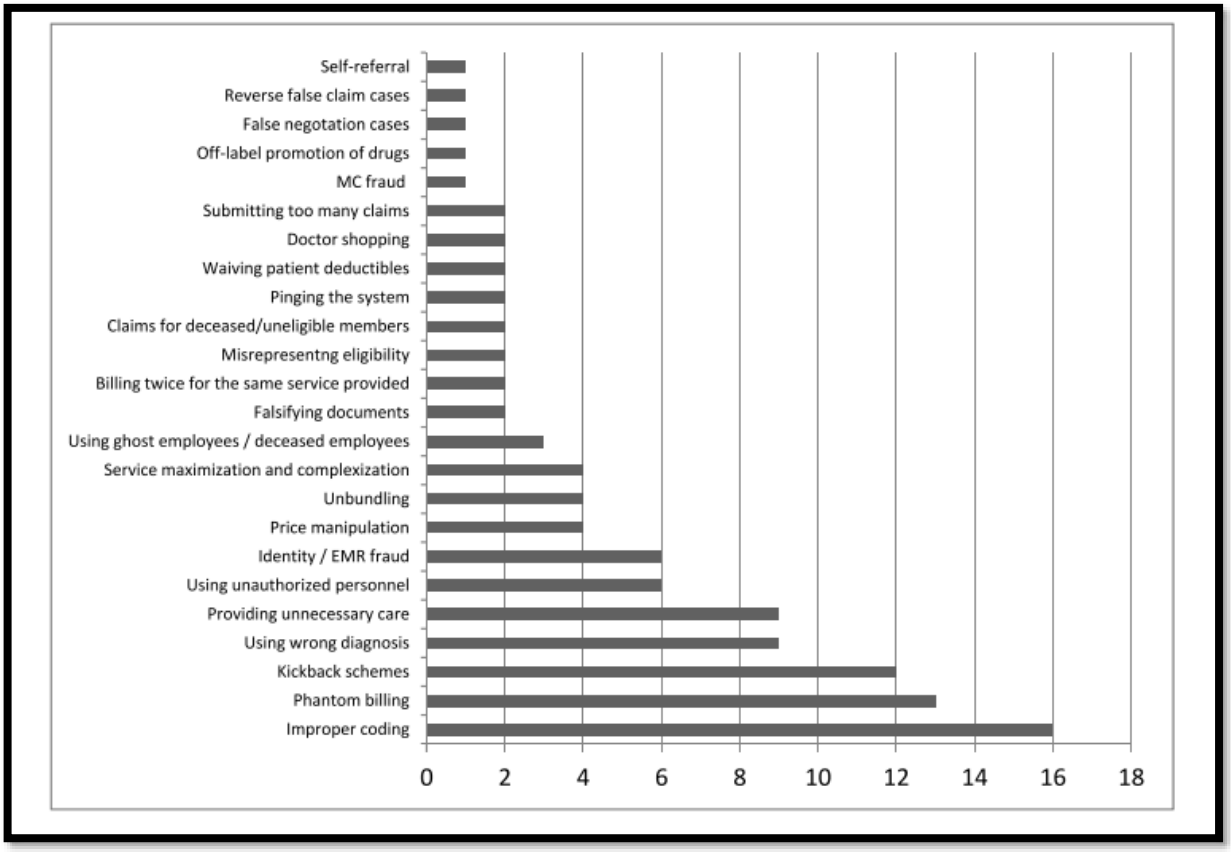
Healthcare fraud is primarily committed by healthcare providers in countries where the government provides health care. In this research, concentration is placed on reducing errors and fraud among private physicians because they are the ones who will benefit the most.

It is vital to understand how healthcare fraud occurs to combat it. The research paper "**Categorizing and Describing the Types of Fraud in Healthcare"**[81] is studied**. T**he above research paper used Webster and Watson's concept matrix technique to evaluate the published literature on various types of fraud. It further categorized and described the

[81] Thornton, D., Brinkhuis, M., Amrit, C., & Aly, R. (2015). Categorizing and Describing the Types of Fraud in Healthcare. Procedia Computer Science, 64, 713–720. https://doi.org/10.1016/j.procs.2015.08.594 Accessed in April 2021

documented types of fraud in healthcare, identified 18 different types of fraud based on the available published literature, and graphically depicted the literature's incidence of health insurance fraud.

Figure 10 Types of fraud in healthcare



Source: (Thornton et al., 2015)

Out of the 18 fraud types identified, the research focuses is on seven fraud types as listed below, which can be addressed by the proposed framework.

Self-Referral

Referring patients to a doctor, diagnostic facility, hospital, or other entity with whom the referring physician has a financial arrangement, is self-referral.

Improper Coding

One of the most often debated and common fraud issues is improper coding, also known as upcoding. It entails charging for a more costly operation or treatment than the one that was done.

Unbundling

Creating independent claims for facilities or supplies bundled together to increase the total billings is known as unbundling. Unbundling can be considered improper coding, but many scholars also mention it as a different form of fraud.

Double Billing/ Multiple Billing

When it comes to filing claims, not only can incorrectly coding procedures be deceptive, but care providers can even threaten to file the same claim several times to get paid again for the same action. The same service is billed several times on the same OHIP.

Billing for services not provided

In double billing, treatment is provided, and the patient is cared for, but the service is billed twice. Claims for healthcare facilities that have not been given and medications and prescriptions that have not been administered to the patient are submitted with bills for services not provided, also termed "Phantom Billing."

Providing unnecessary care and maximizing care

More healthcare may be given than is required to heal the patient, resulting in unnecessary care. Certificates are often falsified to prove the medical necessity of such acts to validate fees. Increasing the number of programs and claimants is a goal. Physician's charge

depending on the number of services they offer under the fee-for-service scheme, so optimizing the number of services means maximizing their billings.

Billing for care provided by people that aren't eligible.

Treatment will be delivered by those who do not have the necessary qualifications or licenses if an intern provides services which he is not licensed to perform or able to charge is an example of this. In this scenario, the practitioner bill for the service on behalf of the intern.

These fraud types are similar to the ten most common healthcare provider fraud schemes mentioned by Charles Piper[82]

1. Billing for services that were not provided.
2. Billing for a service that isn't covered under the plan
3. Misrepresenting dates of service.
4. Misrepresenting locations of service.
5. Misrepresenting a service provider.
6. Deductibles and co-payments are waived.
7. Inaccurate diagnosis or procedure reporting (includes unbundling).
8. Excessive use of services.
9. Corruption, including kickbacks and bribery
10. Prescription drug issuance is either false or unnecessary.

[82] 10 popular health care provider fraud schemes. (n.d.). Retrieved from https://www.acfe.com/article.aspx?id=4294976280 Accessed in May 2021

It is evident that the fraud schemes mentioned above are peddled by some clinics at the physician level and must be monitored from the start to be curtailed. As a result, this research aims to propose a method to limit fraudulent schemes by increasing accountability and transparency, thereby lowering the likelihood of fraud.

Annual General Report 2016[83]

The literature review was focused on OHIP physician billing, and hence, the 2016 Auditor-General Report[84] was researched. It consists of 14 recommendations and 29 actions and some of the pertinent findings regarding physician billings. These findings have been categorized as follows:

Physician Payment Models

- Patient-enrolment models for family practitioner payments are not achieving their goals, and they are causing issues for the Ministry.
    - Physicians in Ontario have consistently been among the highest-paid in Canada. Although one explanation for this is that Ontario has the third-highest population-to-physician ratio, the province still compensates more doctors than other provinces by models such as the patient-enrolment method, which is more costly than fee-for-service. Over the years, doctors have received additional benefits, even though reviews have indicated that some of these payments did not increase the quality of patient care.

[83] Office of the Auditor General of Ontario. (2016). Annual Report 2016. https://www.auditor.on.ca/en/content/annualreports/arreports/en16/2016AR_v1_en_web.pdf Accessed in April 2021

[84] Tabled in the Legislative Assembly of Ontario on November 30, 2016.

- The fee-for-service approach makes it difficult for the ministry to keep expenses under control.
    - In addition, the Ministry is having difficulty handling and monitoring the usage of fee-for-service facilities. One way to save money here is to encourage doctors to eliminate medically unnecessary services.

Physician Billing Mechanism

- Many erroneous physician billings go unnoticed by the Ministry.
- The Ministry does not have sufficient resources in place to reclaim improper fees from physicians.
- Many cases of alleged improper billing by doctors could not be followed up on by the Ministry.

Physician medical liability insurance

- The rising burden of physician medical liability insurance continues to be borne by taxpayers.
    - Physicians' medical liability insurance costs in Ontario have increased dramatically in recent years and are growing. Unlike in the United States, where doctors must pay for their medical liability insurance, all Canadian provinces, including Ontario, refund a percentage of the costs. However, the portion of the cost shared by the Ministry in Ontario is over 87%.
    - The physicians' portion of the contribution remains relatively stable because the Physician Services Agreements have stipulated the amount of the membership fees to be paid by physicians over the last two decades. Because the Ministry pays the

rest, the government responsible for bearing the costs of membership fees increases, and ultimately the taxpayers must bear the rising cost of medical liability protection.

The Auditor-General recommended that the Ministry improve its oversight of fee-for-service payments to physicians by re-establishing an inspector structure, monitoring billings, and establishing a mechanism to recover overpayments, among other things.

In response, the Ministry stated that it had devised a strategy to increase, coordinate, and realign staffing resources to better monitor physician payments. In addition, the Ministry is considering investment options in information and information technology (I&IT) tools to track physician payments and conduct data analysis. It is weighing the costs and benefits of changing the fee-for-service billing review process.

The recommendations from the Ministry further confirm the need for the development of infrastructure to be more transparent with a focus on prevention and detection of fraudulent practices.

News articles on the publishing of Physician billings

Theresa Boyle, a health reporter for Toronto Star, requested the names, specialties, and totals of the province's top-billing doctors at the time.

> **Article 1: Why can't patients see our OHIP billings?**[85]
>
> An itemized invoice is provided for the services not covered under OHIP even before a person leaves the clinic/ office. However, when it's a service covered by OHIP, it is a secret from the patient's perspective as it is at the physician's discretion to bill the patient both in terms of service code and the time of billing.

Within two years, the health ministry was ordered to release the information by Ontario's Information and Privacy Commissioner. However, the Ontario Medical Association (OMA) attempted to overturn the decision, first in Ontario's Divisional Court, then in the Ontario Court of Appeal, and finally in Canada's Supreme Court.

The Supreme Court sided with the Star in April 2019, declining to hear a final appeal, ending the protracted legal battle waged by doctors who wanted the names kept hidden.

[85] Hepburn, B. (n.d.). *Why can't patients see our OHIP billings?* Toronto Star; Toronto Star. Retrieved May 6, 2021, from https://www.thestar.com/opinion/star-columnists/2019/07/10/why-cant-patients-see-our-ohip-billings.html Accessed in April 2021

Article 2: Time to reveal individual MD's OHIP billings[86]

Firstly, the Ministry of Health must follow a years-old directive from the province's former information and privacy commissioner, Brian Beamish, to release physician-identified billing details as soon as possible.

There was a subsequent demand that Beamish's office should respond immediately to another Star details request for the publication of physician-identified billings for all Ontario physicians, which was placed on hold pending the Supreme Court's decision on the top 100.

After the judgment from the Supreme Court which favored disclosure of top 100 billing physicians, the Ministry of Health has provided the information on 194 doctors who appeared in the Top 100 at least once between 2011-12 and 2017-18 fiscal years

Article 3: Transparency on what doctor's bill OHIP[87]

There has been a debate if a fee-for-service structure results in the best medical decisions as there is an inherent incentive to rack up the billable procedures.

In support of the disclosure, it was stated that opening the system to public scrutiny can help build a more robust healthcare system for patients and doctors alike. Greater transparency about OHIP billings benefits the public. It will contribute to

[86] Star Editorial Board. (2019a). *Time to reveal individual MD's OHIP billings*. Toronto Star. https://www.thestar.com/opinion/editorials/2019/04/14/time-to-reveal-individual-mds-ohip-billings.html Accessed in April 2021

[87] Star Editorial Board. (2019b). Transparency on what doctor's bill OHIP informs the health-care debate. *Toronto Star*. https://www.thestar.com/opinion/editorials/2019/06/27/transparency-on-what-doctors-bill-ohip-informs-the-health-care-debate.html Accessed in April 2021

the discussion of how Ontario budgets its healthcare dollars. The amount of money paid to physicians by the provincial government by the Ontario Health Insurance Plan should be made public not only among the top 100 physicians but for all of them. Moreover, this is not a novel concept as doctors' billings are made public in other provinces like British Columbia, Manitoba, and New Brunswick.

Article 4: Increased oversight of OHIP is overdue.[88]

In response to a Kaplan Panel recommendation, the OMA and government are working to find more than $400 million in inappropriate OHIP services. This work is focused on Choosing Wisely Canada (a physician-led group's) discovery that up to 30% of medical services offered in Canada were inappropriate. Suppose Ontario provides a sustainable, publicly funded health system that provides quality services at a reasonable cost. In that case, difficult choices must be taken to ensure that tax funds are used wisely.

In this article, there was an introduction of a new concept of inappropriate services. Shockingly, it is expected to be as high as 30% of the entire medical service.

The demand for the top 100 physicians' billings to be disclosed was aimed at "transparency." However, according to Dr. Ron Linden, the CEO of the Judy Dan Research and Treatment Centre in North York, he has a perfect belief that physicians' billings should

[88] Bob Bell Contributor. (2019). *Increased oversight of OHIP is overdue*. Toronto Star. https://www.thestar.com/opinion/contributors/2019/11/05/increased-oversight-of-ohip-is-overdue.html Accessed in May 2021

not be made public. According to him, the public will misunderstand or misread the publication of physician billings, and the local criminals may target the physicians.[89]

The OMA also argued that the information was kept confidential because doctors were independent contractors rather than government employees whose salaries are subject to disclosure on the Sunshine List. Doctors bear high overhead costs from their billings, so the association was concerned that the public would confuse billings with earnings.

Doctors self-reported average overhead ranging from 12.5 percent in emergency medicine to 42.5 percent in ophthalmology, according to a 2012 article published in the Canadian peer-reviewed journal Healthcare Policy.

According to Marcia Kim, executive director of the Eye Physicians and Surgeons of Ontario, ophthalmologists' overhead costs can be as high as 50% because their equipment must be replaced every five years.

The Ministry of Health does not keep track of these costs. Furthermore, the percentage of overheads varies depending on the level of expertise of each doctor. As a result, publishing the billings of the topmost physicians, i.e., the highest-paid physicians, does not directly address the fundamental issue of transparency.

Even among doctors practicing in the same field, the knowledge, skills, and expertise required to be a doctor cannot be measured or compared. The amount of infrastructure

[89] They're Ontario's top-billing doctors, but for years their identities have been kept secret. Until now - WWWHive. (n.d.). Retrieved from https://wwwhive.com/2019/06/27/theyre-ontarios-top-billing-doctors-but-for-years-their-identities-have-been-kept-secret-until-now/ Accessed in May 2021

necessary to provide the required service and the number of hours spent on service per day are essential contributing factors.

What is required to achieve transparency is not the amount billed by each doctor or physician but rather that the amount billed is only for the provided service.

Our literature review on various types of fraud found in OHIP physician billings encouraged us to preview the two fraud theories and their implications.

Section 2 of the Literature review

Manuals, Reference guides, Specifications

The literature review was undertaken with the available manuals, reference guides, technical specifications from the Ministry of Health for assessing the gap, the scope, and feasibility of implementing Blockchain technology.

The Medical Claims Electronic Data Transfer Reference Manual[90] provides an overview of the MC EDT service, the GO Secure platform, the procedure for uploading claims and downloading various claims reports, and the technical specifications required for physicians or third-party designees to submit an OHIP claim.

Technical Specification for Medical Claims Electronic Data Transfer (MCEDT) Service via Electronic Business Services (EBS)[91]is a reference manual that provides the technical specification intended to aid and guide the development of software that uses the MOHLTC Electronic Business Service (EBS) to access the (MCEDT) web service.

Resource Manual for Physicians[92] is a reference guide for physicians practicing in Ontario that explains how to submit claims and the requirements to connect to MC EDT. It

[90] MOHLTC (2018). Medical Claims Electronic Data Transfer (MC EDT) Reference Manual. https://www.health.gov.on.ca/en/pro/publications/ohip/docs/mc_edt_reference_manual.pdf Accessed in May 2021

[91] MOHLTC (2016). Technical Specification for Medical Claims Electronic Data Transfer (MCEDT) Service via Electronic Business Services (EBS) (p. 35). Ministry of Health and Long-Term Care. http://www.health.gov.on.ca/en/pro/publications/ohip/docs/techspec_mcedt_ebs.pdf Accessed in May 2021

[92] MOHLTC (2017). Resource Manual for Physicians. Ministry of Health and Long-Term Care. https://www.health.gov.on.ca/en/pro/publications/ohip/docs/resource_manual_for_Physicians.pdf Accessed in May 2021

highlights the payment process, review mechanism, recovery, and referral to the Physician Payment Review Board (PPRB), the Accounting Policy and Financial Reporting Branch, or the College of Physicians and Surgeons of Ontario (CPSO) in the event of a conflict between the physician and the General Manager of OHIP.

Blockchain

Recently, there has been a lot of increase in interest in Blockchain technologies. The Blockchain is a cutting-edge cryptography-based transformative technology. The work of Nakamoto in 2008, who demonstrated how this technology would become the central component to facilitate digital currency transactions, was well-known (bitcoin). With the advent of Blockchain, the advantages of this platform would positively affect a variety of fields. Healthcare is one sector where blockchain technologies will be very beneficial.

The Blockchain is also a distributed public ledger for all transactions that eliminates the need for trust between users and the central administrator by distributing power among various computers/nodes in a peer-to-peer (P2P) network.

By concept, a blockchain is a collection of data blocks that record transactions that share specific characteristics. Each transaction using Blockchain technology is registered, time-stamped, and widely publicized with a unique symbol. Transactions are added to the chain of blocks, made up of a unique hash function (an alphanumeric string generated by encoding data using cryptographic private and public keys), a nonce (a unique number for the block), a hash function from the previous block. The genesis block is the first block. As a result, attempting to forge a block necessitates the forging of previous blocks. As a result, the system is stable and protected against attempts to alter a contract.

According to BIS Research, blockchain in the health care system globally will grow to over $5.6 billion by 2025 as more solutions are realized. Furthermore, by 2025, the benefits of blockchain in reducing costs related to data breaches, operations, IT, and fraud are expected to save the industry up to $150 billion per year.[93]

Furthermore, by 2025, the adoption of blockchain in healthcare could save the healthcare industry $100-$150 billion per year in data breach-related costs, IT costs, operations costs, support function costs, personnel costs, and reduce counterfeit fraud products.[94]

Network types of Blockchain.

Blockchain technology platforms can be programmed into two types: public and private. Public (Permissionless) is an entirely public blockchain that anybody can read and write. Private (Permissioned) blockchain that allows various permissions to be assigned to different users on the network. On the blockchain, individual permissions can be needed for different operations.

Private Blockchain with pre-defined users that will act as nodes in claim processing is usable for the healthcare industry.

[93] Digital Disruption: The Transformation of Blockchain in Healthcare. Retrieved from https://healthcareweekly.com/digital-disruption-blockchain-in-healthcare/ Accessed in May 2021

[94] 7 Digital Transformation Trends In Healthcare For 2021 | DAP. Retrieved from https://www.digitalauthority.me/resources/healthcare-trends-2018/ Accessed in May 2021

Smart Contracts

The word "smart contract" was first coined by Nick Szabo in 1997. A smart contract is a programming application that is defined by a Blockchain network address.

A collection of executable functions and state variables make up the smart contract's key components. Each transaction has input parameters that are needed by the contract's purpose. The status of state variables is modified during the execution of a method, depending on the logic implementation.

Standard features in all Blockchains

Blockchain is a digital ledger that, in real-time, is distributed across a network of computers: it is shared, and both users and participants in a peer-to-peer network have access to a copy of the entire record.

A blockchain relies on many network participants to achieve consensus:

Participants use their machines to authenticate and validate each new block before adding it to the existing blockchain. Hence the consensus is vital.

A blockchain uses encryption and digital signatures to confirm identity:

Transactions can be traced back to cryptographic identities, which are technically anonymous but, with some reverse engineering, can be linked to real-life identities.

A blockchain has protocols in place that make it difficult (but not impossible) to alter historical records:

While all data can be read and new data can be written, data from earlier in the blockchain cannot be changed in principle unless the protocol's rules authorize it – for example, by forcing more than 50% of the network to consent to a change.

A blockchain is time-stamped:

Blockchain transactions are time-stamped, making them efficient for tracking and verifying data.

A blockchain can be programmed:

Instructions encoded inside blocks, such as "if" this "then" do that "then" do this, allow transactions or other acts to be performed only if certain conditions are fulfilled and can be supported by additional digital data.

Excellent job explaining the features of blockchain in a clear way that the reader can understand. This could have been extended further by providing an example within the physicians' billings context.

PART 5: Discussion

Introduction

In the literature review, the standard features of Blockchain and Smart Contracts are reviewed. Since the OHIN framework is based on Blockchain technology, the advantages of Blockchain technology and Smart Contracts, in general, are discussed. Blockchain advantages specific to healthcare are then examined. Following this, an OHIN framework with appointment applications and smart contracts is proposed for the fee-for-service reimbursement model in the OHIP physician billing.

Results of the research interview

Mr. David Musyj, President and CEO of Windsor Regional Hospital (WRH) in Windsor, Ontario, Canada, expressed an idea that sparked this research topic. Mr. Musyj was approached during this research and asked for his thoughts on three questions listed in Appendix 3.

Mr. Musyj positively opined that Patients should have the ability to opt-in or out of receiving the OHIP claim information. He further added that the real-time view option is good. Easy access to online claim information will enable the patients to appreciate the services they have received, and the value of those services paid for by the Government.

He drew an analogy between accessing online credit card statements and bank accounts to accessing the Personal Claim History (PCH). Any person can access his monthly billing statement that with username and password; access should be provided to the OHIP claim statement either monthly or in real-time. He wondered if persons could access these as per

their requirements, then how can it be efficient to apply to the Ministry for the Personal Claim information by submitting the form and wait for weeks for a response.

Mr. Musyj further said that the existing method of PCH is not the most user-friendly in 2021, as he attempted to get his PCH statement. It was time-consuming as the process is highly manual as it is necessary to fill out the form entirely and send it via mail or fax. He affirmed that the reply to his PCH application was after few weeks. Additionally, he informed that the report's detail was limited but included dates and a brief description of the service provided.

Regarding the usage of Blockchain technology, Mr. Musyj found the technology fascinating and said that it could be one way a person can safely access his information. The optimum course is to look at the various technologies available to allow residents to access this information safely. He strongly feels that if the technology for the data submission and underlying systems were insufficient, it must be updated as OHIP is a $13+ billion-dollar industry in Ontario alone. He further stated that the cutting-edge technology for tracking submissions, payments/reimbursements, and access should equip the healthcare industry.

Mr. Musyj has come across some who have asked him if access to information will allow possible checks and balances to the overall healthcare system. He has positively replied, giving an example of a credit card statement for the service recipient to verify if they received such service.

Suitability of Blockchain

Blockchain, a distributed ledger system with applications in the energy sector, logistics, banking, and health care, is one technology that can solve these inherent challenges and issues. Blockchain technology allows for safe data storage and transparency, potentially mitigating the chance of healthcare fraud and abuse[95]. Blockchain use cases in health care are starting to emerge, with the primary goal of improving data and process governance.[96]Improved management, sharing, and transmission of patient health data, customer health data, and genomic data are only a few of the critical applications. [97]Many of these applications use blockchain to manage and maintain the privacy of health care records, with an emphasis on patient-focused approaches.[98]

Traditional structures can also achieve the proposed automated event-driven architecture as described under the proposed framework OHIN. However, there are various advantages

[95] Mackey, T. K., Miyachi, K., Fung, D., Qian, S., & Short, J. (2020). Combating health care fraud and abuse: Conceptualization and prototyping study of a blockchain antifraud framework. *Journal of Medical Internet Research*, *22*(9), e18623. https://doi.org/10.2196/18623 Accessed in April 2021

[96]Mackey, T. K., Kuo, T. T., Gummadi, B., Clauson, K. A., Church, G., Grishin, D., Obbad, K., Barkovich, R., & Palombini, M. (2019). "Fit-for-purpose?" - Challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Medicine, 17(1), 1–17. https://doi.org/10.1186/s12916-019-1296-7 Accessed in May 2021

[97] Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability - ScienceDirect. (n.d.). Retrieved from https://www.sciencedirect.com/science/article/pii/S200103701830028X?via%3Dihub Accessed in May 2021

[98] Hylock, R. H., & Zeng, X. (2019). A blockchain framework for patient-centered health records and exchange (healthChain): Evaluation and proof-of-concept study. Journal of Medical Internet Research, 21(8), e13592. https://doi.org/10.2196/13592 Accessed in April 2021

of using Blockchain technology; moreover, since this is cutting-edge technology, it is suitable for the healthcare sector.

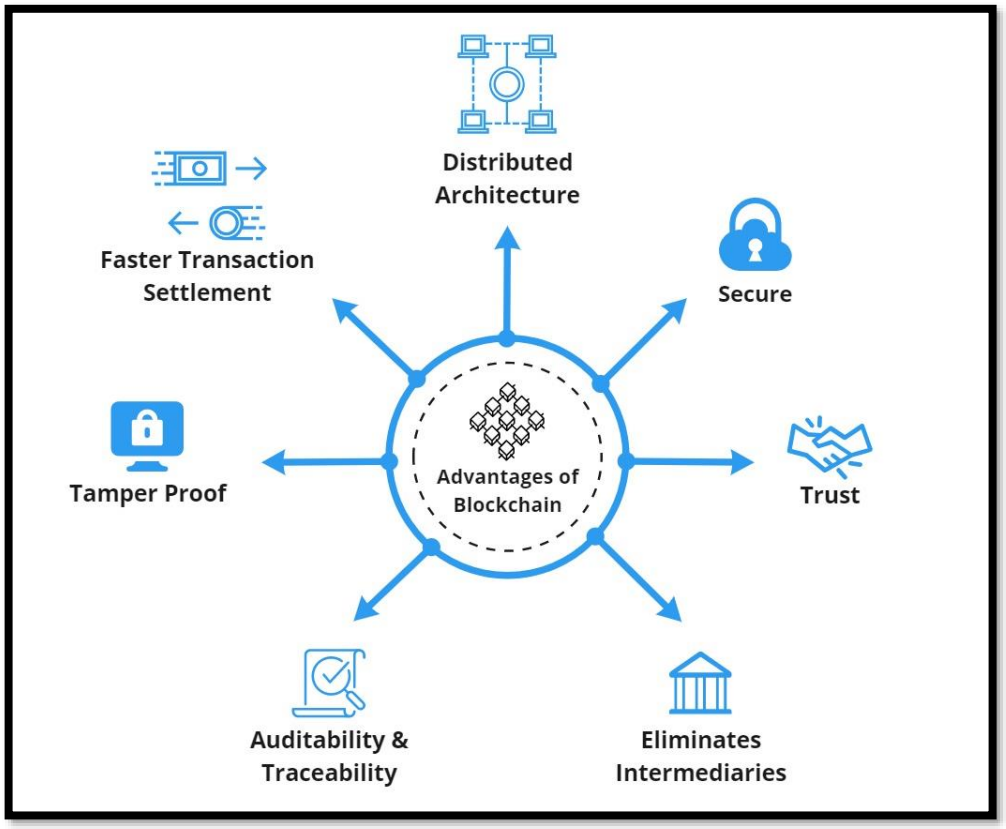
Since the emphasis is on shared validation of claims in a distributed and immutable ledger backed by cryptography, Blockchain was chosen over the other current technology such as cloud computing or conventional database storage methods. Smart contracts could significantly increase confidence in the healthcare claims system by automating the implementation of rule-based reasoning.

For example, if a patient challenges the OHIP physician billing claims under the proposed framework. In that case, a specific response will be immediately triggered, while existing programs require fraud identification and auditing to be done retrospectively. The Smart Contract must be configured according to using the if-then rule.

Integrating blockchain into a system will allow immutability, consensus, incentive creation, and data management in a self-executing system with clear rules through multiple stakeholders.

Advantages of Blockchain Technology

Figure 11 Advantages of Blockchain Technology



Blockchain technology offers many benefits explained as follows:

Distributed Architecture

The main advantage of a Blockchain is that it uses distributed computing technology against centralized computing in conventional methods, which helps it overcome load-sharing issues. Blockchain technology is also reliable for storing various sensitive information such as medical records, patient medical history because distributed computing technology supports graceful degradation.

The distributed architecture eliminates the requirement to store data centrally and allows the decentralization way. As an effective technology for decentralized distributed storage and security management, the blockchain has already shown significant advantages in its application of Bitcoin. Studies have been conducted to understand the application of blockchain technology in various other fields such as vehicle networking[99], especially considering the distributed and secure storage of big data.

The latest blockchain technology used in eHealth introduces fundamental ways to share a distributed view of health-related data and encourages precision medicine, better health, and disease prevention.[100] Blockchain offers a new and promising distributed framework to amplify and support healthcare information integration in various uses and stakeholders.[101]

Secure

When compared to other systems currently in use, blockchain applications provide increased security. Blockchain's security features are critical for ensuring transparency, confidentiality, and fraud protection. It ensures that the appropriate data and information is

[99] Jiang, T., Fang, H., & Wang, H. (2019). Blockchain-based internet of vehicles: Distributed network architecture and performance analysis. IEEE Internet of Things Journal, 6(3), 4640–4649. https://doi.org/10.1109/JIOT.2018.2874398 Accessed in May 2021

[100] Góngora Alonso, S., Arambarri Basañez, J., Lopez-Coronado, M., Arambarri, J., López-Coronado, M., & de la Torre Díez, I. (2019). Proposing New Blockchain Challenges in eHealth Data mining in Mental Health View project IN LIFE Project View project Proposing New Blockchain Challenges in eHealth. Article in Journal of Medical Systems. https://doi.org/10.1007/s10916-019-1195-7 Accessed in April 2021

[101] Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2018). Blockchain-Based Medical Records Secure Storage and Medical Service Framework. Journal of Medical Systems, 43(1), 1–9. https://doi.org/10.1007/s10916-018-1121-4 Accessed in May 2021

available to the right people, whether internal or external, at the right time, in the right place, and through the right channel. Security protects enterprise data assets by securing and encrypting data in motion and, at rest, preventing and thwarting malicious attacks. It also allows businesses to separate roles and responsibilities, ensuring that sensitive data is protected without jeopardizing privileged user access. The one-way hash function is a mathematical function that converts a variable-length input string into a fixed-length binary sequence used by the Blockchain network. The output does not appear to be related to the input. The process is difficult to reverse because the input cannot be determined from the output alone.[102]

A study discussed that using a proposed blockchain-based information management system to handle patients' information, such as electronic medical records (EMRs), also exhibits high information security combining the customized access control protocols and symmetric cryptography. This technology can play a significant role in the sharing of sensitive medical data.[103]

Trust

Blockchain technology ensures that records are kept securely and that a shared process is followed. The most critical issue in the Blockchain is trust. The interactions between the network's nodes ensure that trust is established. Instead of relying on trusted third-party

[102] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on Blockchain technology? - A systematic review. PLoS ONE, 11(10), e0163477. https://doi.org/10.1371/journal.pone.0163477 Accessed in May 2021

[103] Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. Journal of Medical Systems, 42(8). https://doi.org/10.1007/s10916-018-0993-7 Accessed in May 2021

organizations to facilitate transactions, Blockchain network participants rely on the Blockchain network itself. The rise of the significant data era on the Internet had also resulted in a massive increase in data size. However, the most severe problem with big data is a lack of trust, making it difficult for safe data circulation and industry development. By integrating non-tampering, traceable attributes with smart contracts which automatically execute default instructions, Blockchain technology offers a new solution to this problem.[104]

Blockchain implementations convey trust because of their decentralized and immutable nature, as well as their transparency. Smart contracts, or additional rules, can be inbuilt into the decentralized, immutable, private, and trusted ledgers to control how the data is used. Smart contracts aren't a standard feature of every blockchain, but they're crucial in the complicated world of healthcare.[105]

Eliminated Intermediaries

By eliminating intermediaries, higher efficiency and speed would be achieved and a significant decrease in settlement time. Since Blockchain technology is a decentralized system, it does not require collaboration with a third-party organization or a central administrator. It indicates that the process operates without using an intermediary, with all participants in the Blockchain making decisions. The database security process usually

[104] Weber, I., Gramoli, V., Ponomarev, A., Staples, M., Holz, R., Tran, A. B., & Rimba, P. (2017). On availability for blockchain-based systems. Proceedings of the IEEE Symposium on Reliable Distributed Systems, 2017-Septe, 64–73. https://doi.org/10.1109/SRDS.2017.15 Accessed in May 2021

[105] Engelhardt, M. A. (2017). Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. Technology Innovation Management Review, 7(10), 22–34. https://doi.org/10.22215/timreview/1111 Accessed in April 2021

takes a long time and costs a lot of money, but Blockchain technology aids in avoiding this expense.[106]

Blockchain is the checking mechanism that facilitates and verifies transactions. Because blockchain acts as a checking mechanism, this self-regulation removes the human element, commonly referred to as the middleman. This removal benefits from streamlining the contracting process, lowering the likelihood of human error, and creating a more cost-effective option.[107]

Improved traceability

Blockchain technology is a distributed network of data. This technology provides tamper-proof data with solid authentication where the information about all the products is encrypted. It helps avoid inevitable consequences like non-transparent in nature, interference in supply chain management, or logistics.[108] An example from the farming industry, Blockchain technology, enables creating a more competent and secure supply chain by providing a real-time audit trail of the tracked products.

---

[106] Engelhardt, M. A. (2017). Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. Technology Innovation Management Review, 7(10), 22–34. https://doi.org/10.22215/timreview/1111 Accessed in May 2021

[107] Young, C. R. (n.d.). A Lawyer's Divorce: Will Decentralized Ledgers and Smart Contracts Succeed In Cutting Out the Middleman? (Vol. 96). Retrieved from https://openscholarship.wustl.edu/law_lawreview Accessed in May 2021

[108] Madumidha, S., Ranjani, P. S., Varsinee, S. S., & Sundari, P. S. (2019). Transparency and traceability: In food supply chain system using blockchain technology with internet of things. Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI 2019, 983–987. https://doi.org/10.1109/ICOEI.2019.8862726 Accessed in May 2021

The Blockchain's transparency is achieved through the transaction copying process. Each transaction is copied to all computers in the Blockchain network. Every participant can look at all transactions, which means that each action is shown to participants of the Blockchain. Nobody can do anything insensibly. It ensures secure and transparent access to the medical records of each patient in the medical institution[109]

Auditability

Each transaction is recorded in the Blockchain network, which ensures the asset's audibility between two parties. It's beneficial for companies that need a data source to authenticate assets. The Blockchain format is designed so that any problem can be quickly identified and corrected if necessary. It also leaves a permanent audit trail. A significant benefit of a Blockchain solution is the combination of decentralization and a tamper-proof process history that facilitates audit.

Tamper Proof

A distributed ledger that stores linked blocks of transactions is known as a blockchain. Unlike the other system level, blockchain helps to ensure that approved transactions are securely stored. The ability to create, store, and transfer digital assets in a distributed, decentralized and tamper-proof manner is advantageous. It will not be possible to change or delete a transaction once connected to the Blockchain when a decentralized system, such as the Blockchain, each transaction linked to it is copied to every computer in the

[109] Demestichas, K., Peppes, N., Alexakis, T., & Adamopoulou, E. (2020). Blockchain in agriculture traceability systems: A review. Applied Sciences (Switzerland), 10(12), 1–22. https://doi.org/10.3390/APP10124113 Accessed in May 2021

Blockchain network. As a result of this benefit, Blockchain technology is unchangeable and unbreakable.[110]

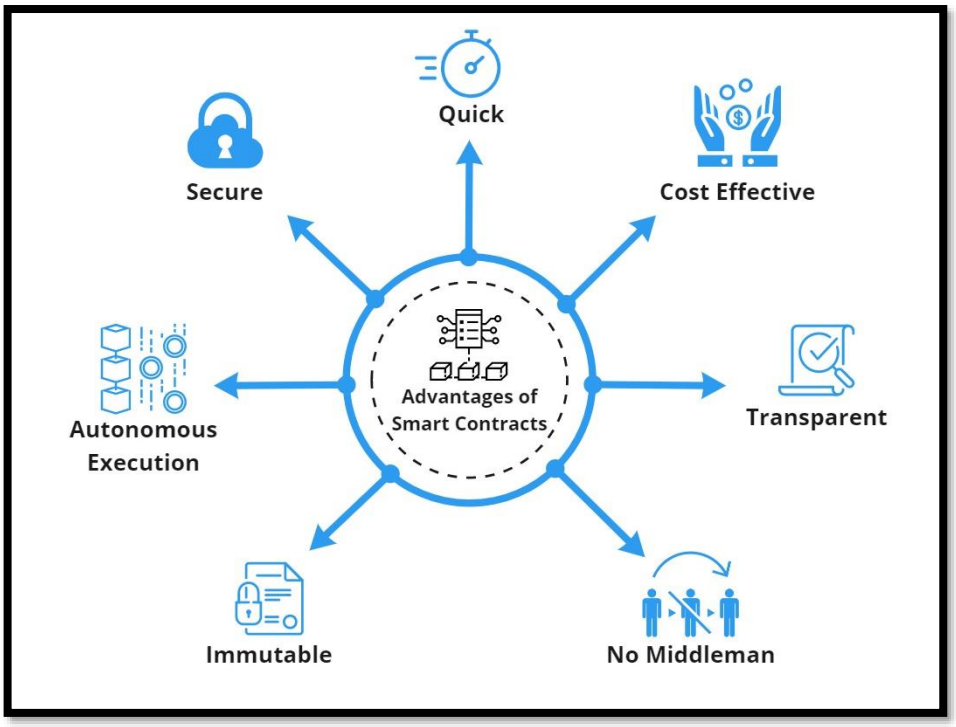
Faster Transaction settlement

Traditionally, processing and initializing a transaction into any organization, such as banking or agricultural food supply, takes a long time. The use of Blockchain technology reduces the time required for processing and initialization.

[110] Demestichas, K., Peppes, N., Alexakis, T., & Adamopoulou, E. (2020). Blockchain in agriculture traceability systems: A review. Applied Sciences (Switzerland), 10(12), 1–22. https://doi.org/10.3390/APP10124113 Accessed in May 2021

Advantages of Smart Contracts

Figure 12 Advantages of Smart Contracts



Quick

Manually processing paperwork and documents in a traditional contract takes a long time. Smart contracts use code to automate tasks, saving hours in many business processes. Smart contracts, in essence, do not require human intervention and are guided and monitored by other nodes in the blockchain network. As a result, the scripted contract self-executes once the contract is triggered. When scripting the contact, this is frequently accomplished by using trigger events. Each contract is treated as a distinct entity, and each transaction, regardless of its source, is validated first. Overall, this results in a contract execution process that is quick, dependable, and secure.

Cost-effective.

Without going through a mediator, blockchains ensure the trust of the entire system through distributed consensus mechanisms. In a decentralized manner, smart contracts stored in blockchains can be automatically triggered. The administration and service costs incurred due to the third-party intervention can be significantly reduced. Because a smart contract system does not require an intermediary, overhead and transaction costs are reduced considerably.

Autonomous Execution

Smart contracts function as self-contained actors whose actions are entirely predictable. A smart contract is a self-enforcing nature. However, self-sufficiency has a different emphasis. A smart contract does not need any legal institutions to exist, neither enforcement agencies nor the corpus of legal rules, default or mandatory ones to supplement it as they do about classic contracts in case of their incompleteness. A smart contract is a software code implemented on the Blockchain platform. It ensures the self-enforcing and autonomous nature of its terms triggered by pre-defined conditions and applied to Blockchain titled assets.

Security with Smart Contracts.

Smart contracts implemented through blockchain technologies entails the use of decentralized network made of non-trusting parties. The fact that the parties in the network are non-trusting makes them keep check of one another to ensure each transaction is carried out effectively and that there is a uniform world view of the status of all the transactions. Again, blockchain technology is implemented through cryptography techniques. This

technology entails high encryption of data and the use of both private and public keys for reading the transactions in each blockchain and executing any transaction. Before any node commits a transaction, the transaction must first be validated by all the odes across the blockchain network to enhance the security of the smart technology[111] The encoded contract clauses in smart contracts are stored in blockchain. Only the contract parties can access contract clauses, so changing the code respectively modifying the contract conditions is impossible. As a result, smart contracts establish a secure and private environment, resulting in reducing contract fraud.[112]

Immutable

An important aspect of smart contracts is that they are immutable (once deployed, the smart contract's code cannot be changed), which ensures that no one can change the behavior of the smart contract, protecting users from malicious changes[113]. Due to cryptographic techniques, blockchain is immutable and auditable, providing an uncensored source of truth. Smart contracts can also be stored on blockchains. Once a contract is published to the network, it will perform exactly as specified without additional input or maintenance. There is no way for a smart contract's operation to produce unexpected results or to be compromised. Because a blockchain is a distributed, immutable ledger, it allows for easy

[111] Allam, Z. (2018). ON SMART CONTRACTS AND ORGANISATIONAL PERFORMANCE: A REVIEW OF SMART CONTRACTS THROUGH THE BLOCKCHAIN TECHNOLOGY. 11(2), 137–156. https://doi.org/10.1515/rebs-2018-0078 Accessed in May 2021

[112] Ahmadisheykhsarmast, S. (2018). Smart Contracts in Construction Industry. https://www.researchgate.net/publication/329363162 Accessed in May 2021

[113] Pace, G. J., Ellul, J., & Azzopardi, S. (2018). Monitoring Smart Contracts: ContractLarva and Open Challenges Beyond. https://www.researchgate.net/publication/327834131 Accessed in May 2021

auditing of all transactions on a (business) network. The bottom line is that the immutability of the environment in which smart contracts are executed can revolutionize the way parties settle legal disputes.[114]

No Intermediary

The use of blockchain technology to implement smart contracts eliminates the need for a middleman and aids in reducing overall organizational costs and maximizing profit margins. A smart contract's performance is always mediated by technology. The technological platforms govern payments and other actions within contractual clauses with rules-based operations. Essentially, the middleman is no longer necessary. The elimination of the dependence on the intermediary can significantly improve the efficiency of the business process. For example, in the supply chain, the financial settlement will be automatically completed in a peer-to-peer manner once the predefined condition is met. As a result, the turnaround time can be significantly reduced[115].

Transparency

Smart contracts are generally not complex, which improves their transparency. Smart contracts execute on complex infrastructure, the backbone of the Blockchain, a globally replicated data structure available for public scrutiny that contributes to the transparency of the infrastructure. Users must be able to inspect the server and vice versa to assess the

[114] Gilcrest, J., & Carvalho, A. (n.d.). Smart Contracts: Legal Considerations. Retrieved from http://coinmarketcap.com Accessed in May 2021

[115] Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., & Imran, M. (2019). An Overview on Smart Contracts: Challenges, Advances and Platforms. Future Generation Computer Systems. https://doi.org/10.1016/j.future.2019.12.019 Accessed in April 2021

transparency of the client. Current blockchain explorers provide insufficient support for such inspections[116]. A study conducted showed that smart contracts running on the Ethereum blockchain could improve the transparency of data management in clinical trials. It showed that smart contracts could act as trusted administrators, enhance the transparency of data reporting in clinical trials, and capture all aspects of data that might be subject to manipulation.[117]

In the case of Smart contracts, the terms and conditions of the contract terms and conditions become explicitly visible to the different network players of the specific blockchain. Therefore, once the contract is established, changes cannot be easily implemented. Each transaction by either party to the contract is monitored and controlled by other network nodes in the blockchain. As a result, transparency is promoted, and issues of fraud are eliminated[118]

[116] Hartel, P., & Mark Van Staalduinen, |. (n.d.). ARTICLE TYPE Truffle tests for free-Replaying Ethereum smart contracts for transparency. Retrieved from http://truffleframework.com Accessed in May 2021

[117] Nugent, T., Upton, D., & Cimpoesu, M. (2016). Open Peer Review Improving data transparency in clinical trials using blockchain smart contracts [version 1; peer review: 3 approved]. https://doi.org/10.12688/f1000research.9756.1 Accessed in May 2021

[118] Ibid

Blockchain advantages in the healthcare sector

The concept of using Blockchain in healthcare was inspired by the need for security and interoperability in healthcare and the need to manage the privacy of patient data.[119] Blockchain technology can provide a solution that secures the recording and exchange of medical data and ensures each patient's data integrity by giving patients control over their personal information.

- Some of the benefits that have been identified for 'People'[120] who use Blockchain technology are that it enables interoperable, unified, and secure views and exchanges of electronic health records. Patients have the right to own their medical records. Up-to-date data is available when needed. Moreover, Authorities may be able to use blockchain technology to gain access to health data as needed.
- The benefits of Using Blockchain Technology in 'Processes'[121] are that since Blockchain technology has a high level of tamper resistance, vulnerable health data can be guaranteed to be stored in a secure environment. Claims authentication, eligibility checks, and preauthorization can all be automated with Blockchain, improving the process's reliability, validity, performance, and security.

[119] Alla, S., Soltanisehat, L., Tatar, U., & Keskin, O. (2018). Blockchain Technology in Electronic Healthcare System Curriculum Development-Blockchain Technology for Cyber Security View project Blockchain Technology View project Blockchain Technology in Electronic Healthcare Systems. https://www.researchgate.net/publication/325542378 Accessed in May 2021

[120] Ibid.

[121] Ibid.

- Some benefits of using Blockchain regarding 'technology'[122] are that blockchain technology architecture is flexible, adaptable, agile, and secure, with high efficiency and low latency.

In the healthcare industry, security is a significant concern. Many patient records being exposed in security breaches have been reported in the United States in recent years. Because blockchain can keep an incorruptible, decentralized, and transparent log of all patient data, it's ready for security applications[123]. The technology's decentralized nature creates a single ecosystem of patient data that doctors, hospitals, pharmacists, or anyone involved in treatment can access quickly and efficiently.

In many healthcare applications, blockchain technology is trying to redefine data modelling and governance. It is predominantly due to its ability to segment, secure, and share medical data and information unprecedentedly. Blockchain technology is at the heart of many current healthcare developments. Blockchain technology is expected to alter the healthcare ecosystem and improve the security and quality of healthcare. The use of blockchain in health data management applications empowers patients and facilitates sharing of health data.[124]

---

[122] Alla, S., Soltanisehat, L., Tatar, U., & Keskin, O. (2018). Blockchain Technology in Electronic Healthcare System Curriculum Development. Retrieved from https://www.researchgate.net/publication/325542378 Accessed in May 2021

[123] 15 Top Blockchain in Healthcare Examples Helping Revive the Industry 2021 | Built In. Retrieved from https://builtin.com/blockchain/blockchain-healthcare-applications-companies Accessed in May 2021

[124] Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. Applied Sciences (Switzerland), 9(9), 1736. https://doi.org/10.3390/app9091736 Accessed in May 2021

Currently, the healthcare industry is looking to take advantage of emerging technological advancements to provide the best possible services and solutions. Amongst various technologies, Blockchain technology has an excellent potential to transform healthcare. It has the potential to assist the healthcare industry in overcoming its current challenges. It can help with universal access, integrity, security, traceability, and interoperability.[125]

Blockchain healthcare applications are critical to improving the current state of healthcare. Drug prescription, lab test results, patient medical records, claim, and billing is some of the blockchain use cases in healthcare. In these cases, blockchain technology has aided in the resolution of various problems and issues. Healthcare billing and claims, for example, are riddled with fraudulent activity, with billing bearing the brunt of the damage. Blockchain technology can automate both the billing and claim processes. If the billing process is linked to the Blockchain, there is no way for a health care provider to overcharge a patient or add a service that the patient never requested in the first place.[126] It can also improve the management of claims that can be done in minutes rather than months. Since Blockchain eliminates intermediaries, automation will take control of the entire claim process.[127]

Blockchain can play a significant role in shaping the future of technologies in healthcare in the coming years. Its usage is as follows

- use of data in clinical research;
- identity protection for the users here, the patients, and the healthcare providers;

[125] Blockchain For Healthcare: Use Cases And Applications | 101 Blockchains. Retrieved from https://101blockchains.com/blockchain-for-healthcare/ Accessed in May 2021
[126] Ibid
[127] Ibid

- managing pharmaceutical and medical device supply chains;
- maintaining the public health;
- reducing medical-related fraud, especially claim management.

Amongst other technology, Blockchain is a strong contender in reshaping the global healthcare landscape.[128]

Health Care Service Corporation (HCSC), PNC Bank (NYSE: PNC), and IBM (NYSE: IBM) recently announced a partnership to design and build a blockchain technology network to improve healthcare transparency and interoperability. They want to build a blockchain network that will benefit multiple members of the healthcare ecosystem by providing a safe, shared environment.[129]

'Guardtime' and partners have launched the world's first blockchain-supported Personal Care Record Platform to up to 30 million NHS patients in the United Kingdom. According to estimates, the 'MyPCR' platform will improve medication adherence and save at least £800 million in the UK and $290 billion in the US.[130]

'Rajasthan Healthcare 3.0' is the first state in India to successfully implement the Electronic Health Records on Blockchain in 2018.[131]

---

[128] Kamel Boulos, M. N., Wilson, J. T., & Clauson, K. A. (2018). Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare. In *International Journal of Health Geographics* (Vol. 17, Issue 1, p. 25). BioMed Central Ltd. https://doi.org/10.1186/s12942-018-0144-x Accessed in May 2021

[129] 7 Digital Transformation Trends In Healthcare For 2021 | DAP. Retrieved from https://www.digitalauthority.me/resources/healthcare-trends-2018/ Accessed in May 2021

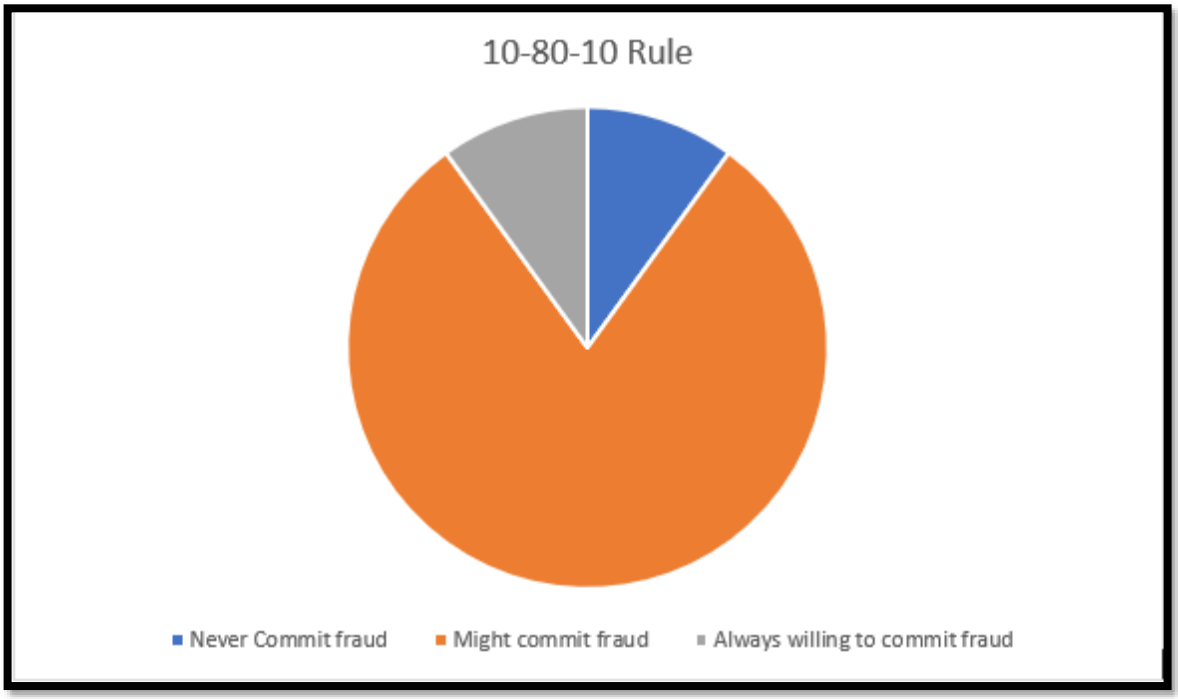
[130] Ibid

[131][131] https://digitalindia.gov.in/writereaddata/files/Rajasthan.pdf Accessed in May 2021

Proposed Framework: Ontario Health Insurance Networks (OHIN)

The OHIN framework is based on Cressey's Fraud Triangle, which relies on the three interconnected elements of pressure, opportunity, and rationalization to enable someone to commit fraud. Fraud risk is the risk from persons capable of combining all three of these elements. As per the study**, 80 %** of the population might commit fraud given the right combination of opportunity, pressure, and rationalization.[132]

Figure 13 Fraud: 10-80-10 Rule



In the proposed framework, emphasis is laid on reducing the opportunity element in the OHIP physician billing, which is an element that can be controlled along with Capability, as explained in the Fraud Diamond theory.

[132] Source: National Association of State Auditors, Comptrollers and Treasurers (NASACT) and the Oregon State Controller's Division

The framework is designed to strengthen the anti-fraud controls within the OHIP billings and focus on efficiency and transparency in the OHIP claim process based on the following principles.

Enhancing the Detection Perception

Most experts agree that preventing fraud is far easier than detecting it. It is vital to know something about the mindset of the potential perpetrator to avoid fraud. The most effective fraud prevention method may be to increase the perception of detection. Controls, for example, are useless in preventing theft and fraud if those at risk are unaware of detection.

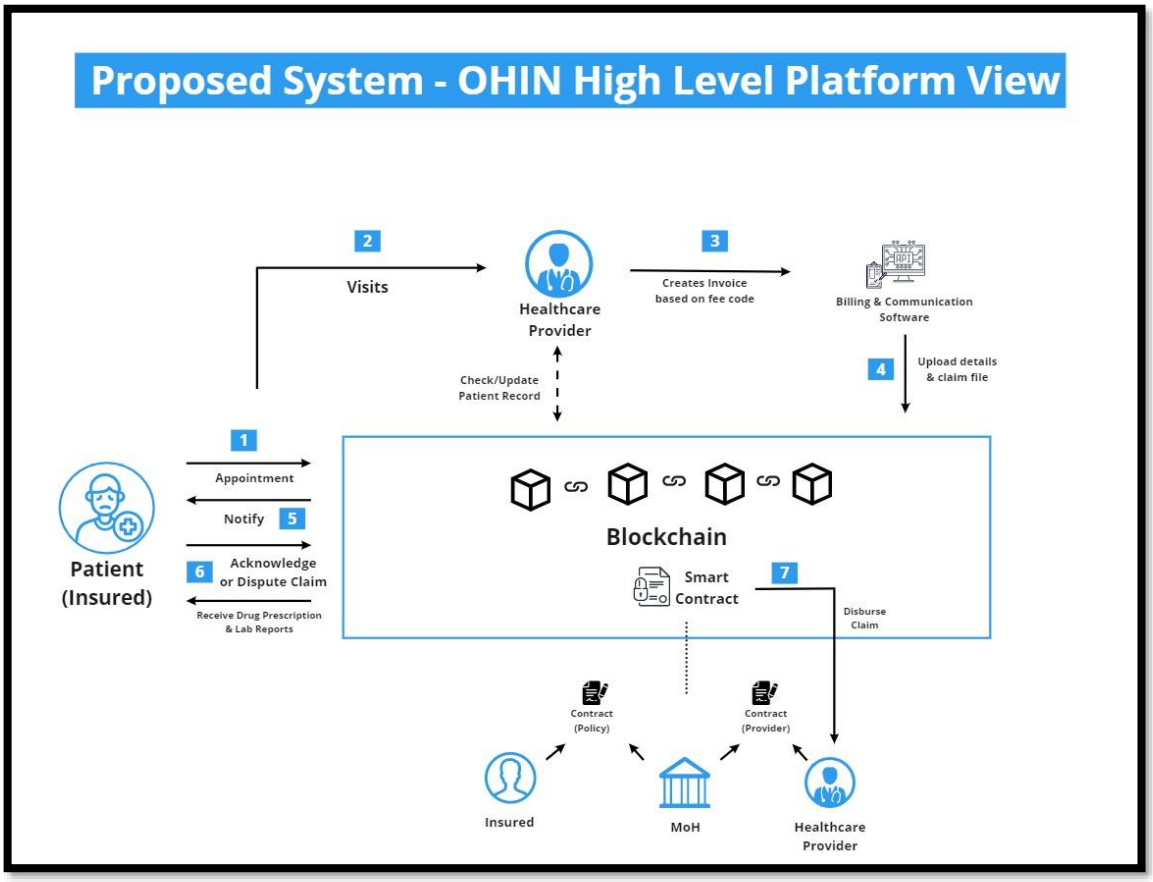
Procedures for Proactive Auditing Mechanism.

Instead of waiting for instances to happen, proactive audit procedures demonstrate the Ministry's intention to seek out possible fraudulent conduct aggressively. Smart contracts can embed analytical review, fraud assessment questioning, and surprise audits, where possible.

Enhancing the transparency in the OHIP Physician billing.

The possibility of the audit trail deters the desire to commit fraud. The proposed framework will keep track of any claim from the appointment event to the reimbursement event. Hence transparency can easily detect any fraudulent claims. A technological architecture for a blockchain-based solution that incorporates three core stakeholder groups in the OHIP physician billing process to allow a more proactive system based on the above-stated common elements and advantages is introduced. This research paper would explore the usefulness of blockchain by creating a technical design framework for combating OHIP physician billing fraud.

Figure 14 Proposed Framework: Ontario Health Insurance Network (OHIN)



Process with OHIN

When a patient needs to meet a doctor, the appointment transaction is the first step in the proposed OHIP claim process, and it will start a chain of events with an audit trail from the appointment to the visit, the claim submission, and the claim payment.

A visit transaction, for example, involves a patient and a physician; a prescription transaction consists of a patient, the prescribing physician, and eventually the pharmacist who fills the prescription medication; and a laboratory examination transaction involves a patient, the referring physician, and the laboratory representative. Since OHIP physician claims are the focus of the proposed framework, the parties involved are health care

providers for claim initiation, patients for claim viewing and escalation if a discrepancy is discovered, and the MOH agency for claim validation.

The required participants must sign the transactions using a suitable collective signature protocol. There will be a small number of signing parties in most cases, and the signing process will be quick.

Transactions

Under the proposed system Ontario health insurance network, the ***first Transaction*** is the appointment by the patient. The appointment process is explained in Figure 16.

The ***next Transaction*** would be a patient visiting a healthcare provider for treatment. The healthcare provider will see the patient, provide treatment, give the lab requisitions or the drug prescriptions, or even suggest a visit to a specialist.

Transaction 3 would then be for the healthcare provider to create the invoice using the billing and the communication software provided by the Ministry.

Transaction 4 would be for the healthcare provider to upload the OHIP claim on a Blockchain-enabled platform. The lab requisitions and the drug prescriptions are to be uploaded by the doctors to complete a claim.

Transaction 5 will be automated intimation of the claim to the patient. The history of the claim will be available in the patient's portal login. A text message will enable real-time intimation when the healthcare provider or their designates upload the claims.

Transaction 6 will for the patient to either agree to the service or dispute it through the portal or message. Once the patients acknowledge the claim in either manner, they will

receive the lab requisition or the drug prescription. It will act as a motivator for the patient to recognize the event. Suppose the patient does not acknowledge it within 24 hours of upload. In that case, the default mechanism will process the claim and proceed for payment on the honour system until any automated check extracts it for detailed review or audit.

Transaction 7 is a Smart Contract in-built with the platform. It will enable the transaction log and the audit trail from the patient booking for an appointment, the appointment is granted, the patient visiting the healthcare provider, and finally, the invoicing from by the healthcare provider for the service provided. The Smart Contract working within OHIN is explained in Figure 17.

The healthcare provider will be reimbursed directly to the pre-defined bank account when all these events are genuinely and correctly performed under the smart contract.

Since all these transactions are built on a blockchain platform, the healthcare provider and the patient can access these transactions using user-specific credentials. As real-time processing is possible, it will reduce the risk of the patient losing track of the service provided regarding the nature, date, and place of service.

If the patient escalates the matter, it raises a red flag to trigger the audit mechanism. Similarly, variation in patterns and testing of validation rules that are pre-determined based on the time, geography, or nature of service or the treatment provided by the physician to his patients over some time can activate an audit.

The automated rules and coding within the Blockchain platform will generate these exceptional reports.

Proposed Concept of OHIN

The Blockchain technical framework is designed for OHIP physician billing using leading blockchain solutions and application layers such as consensus algorithms, smart contracts, tokens, and governance based on digital identities.

The technological backbone for OHIN based on Blockchain technology, including key solution design principles, solution architecture, IT Strategy, and the Information Security framework required for the OHIN, is shown in Appendix 1.

Our blockchain framework aims to facilitate a shared governance approach to tackling the OHIP physician billing fraud while also giving patients the option and authority to participate actively in the claims review process.

Reliance is placed on the Fraud Diamond theory and tried to reduce the opportunity and the capability component from the OHIP claim process while designing the OHIN. The fundamental design theory of OHIN is based on two main facts:

1. Patients are best suited to verify whether appropriate health care services have been rendered by the healthcare provider with the OHIP claims, and
2. Patient verification or lack of verification of claims is an essential indicator of potential OHIP physician billing fraud risk, which the investigation can later confirm.

This process can also allow targeted fraud prevention that is more proactive than conventional fraud prevention.

As a result, this approach emphasizes a patient-focused design to combat OHIP physician billing fraud by including patients as core stakeholders in the claims review process.

The OHIP bills raised by the healthcare provider can be confirmed by the patient, even if it is not the same service, as this will reduce the possibility of billing for the wrong service, incorrect dates, time, or double billing. However, upcoding and unbundling, on the other hand, will be challenging to address because patients will be ignorant of the technical requirements for billings.

Establishing interest in a shared governance approach through various stakeholders in the same transaction is central to this framework. It allows the patient to serve as an additional node to view the claims on a real-time basis.

Blockchain infrastructure is suitable for this use case because of these critical features and the technological application layers provided by blockchain (e.g., smart contracts, digital identity, tokens, and consensus mechanisms).

Blockchain increases the authentication and data privacy of data contained in a system. When deciding whether a blockchain is a suitable technology for a given issue, properties such as public verifiability, transparency, privacy, integrity, redundancy, and trust are considered.

Consortium permissioned blockchain[133] is used, which seemed like a suitable technological approach to address the challenges faced by the existing OHIP billing process.

[133] Hylock, R. H., & Zeng, X. (2019). A blockchain framework for patient-centered health records and exchange (healthChain): Evaluation and proof-of-concept study. *Journal of Medical Internet Research*, *21*(8), e13592. https://doi.org/10.2196/13592 Accessed in April 2021

Furthermore, smart contracts on the blockchain allow for the automated execution of an agreed-upon rule collection in response to incidents. The focus is on Fee-for-Service physician billing. Hence, the "Schedule of Benefits" as negotiated by the Ministry and OMA will be the vital element in designing the business rules of the smart contract.

Proposed Architecture of OHIN

The proposed OHIN framework consists of various stakeholders who will access the Ontario Health Insurance Network through independent hardware systems connected through the Internet. Since the login is password protected, it will provide the first line of defence against unauthorized access.

Individual users must log in to their respective systems/devices to create, record, validate or view OHIP claims while interacting appropriately with other stakeholders in the framework.

All the stakeholders, such as healthcare providers, medical practitioners, and patients, an agency from MOH must be explicitly authorized to access and use the system. This authorization process is critical as a private permissioned blockchain that operates within predefined stakeholders is used. A central authority, in this framework, the Ministry of Health, which certifies healthcare practitioners, will also provide authorization to submit claims and are responsible for payment of claims once the Smart Contract condition is fulfilled.

The three-step registration procedure for any healthcare practitioner to be able to submit OHIP claims is briefly outlined below:

1. Before applying for an OHIP billing number, a new physician (or a physician new to Ontario) should obtain an Independent Practice License. This license is a five-digit number that identifies the physician as a member of the College of Physicians and Surgeons of Ontario (CPSO) and allows them to practice medicine independently and unsupervised in Ontario.
2. The physician must then apply for an OHIP billing number, a six-digit number that tells the Ministry of Health (MOH) who submitted the claims and from where such claims were submitted.
3. The physician must then sign up for GO Secure, Medical Claims Electronic Data Transfer (MC EDT), and Health Card Validation (HCV).

Once all these registrations are complete, a healthcare provider who can practice independently will be authorized by the Ministry of Health to become the stakeholder in the OHIN.

All residents of Ontario are covered by the Ontario Health Insurance Plan, which covers essential health services; additional services may be covered by individual or group insurance contracts. In this research, only claims related to OHIP physician billings are dealt with within this framework. Patients can get auto-registered to view the blockchain-based system during the first appointment with the healthcare provider, which is the first step in the Ontario Health Insurance Network (OHIN). For their subsequent visits, the same credentials can be used to access the OHIN.

Because Ontario has a government-sponsored universal healthcare system, such a software system for patients can be run by the Ministry of Health's agency. The Ministry of Health in Ontario already has agencies that store patient based OHIP physician claims accessible

to patients through the ministry portal's Patient Claim History (PCH) facility. Furthermore, patients already have identification cards in the form of a Health Card to verify the user's identity. The critical distinction is that the proposed framework must include mechanisms that allow patients to easily access their claim data, possibly on a real-time basis, just like any commercial merchant transaction.

The Ministry of Health would play a key role in certifying healthcare providers, patients, and the agency within the Ministry that handles OHIP physician billing claim settlement.

Fraud in OHIP costs the Ministry of health and indirectly the taxpayers a fortune, mostly because regular procedures centred on publicly available data and proprietary data sources are incapable of detecting fraudulent activities. The proposed framework emphasizes a patient-focused approach that seeks to give patients greater transparency and control over the claims made by the physicians on their Health cards.

It also ensures that patients are recipients of the claims data and can respond in the case of a discrepancy.

Conventionally, health care fraud prevention has been applied by reactive mechanisms that analyze suspicious claims conduct after a claim has already been made and paid is also central to the research methodology. Traditional programs can be expensive (because the amount defrauded can never be retrieved or needs lengthy litigation). They rarely include patient input when validating the credibility of the OHIP physician claim.

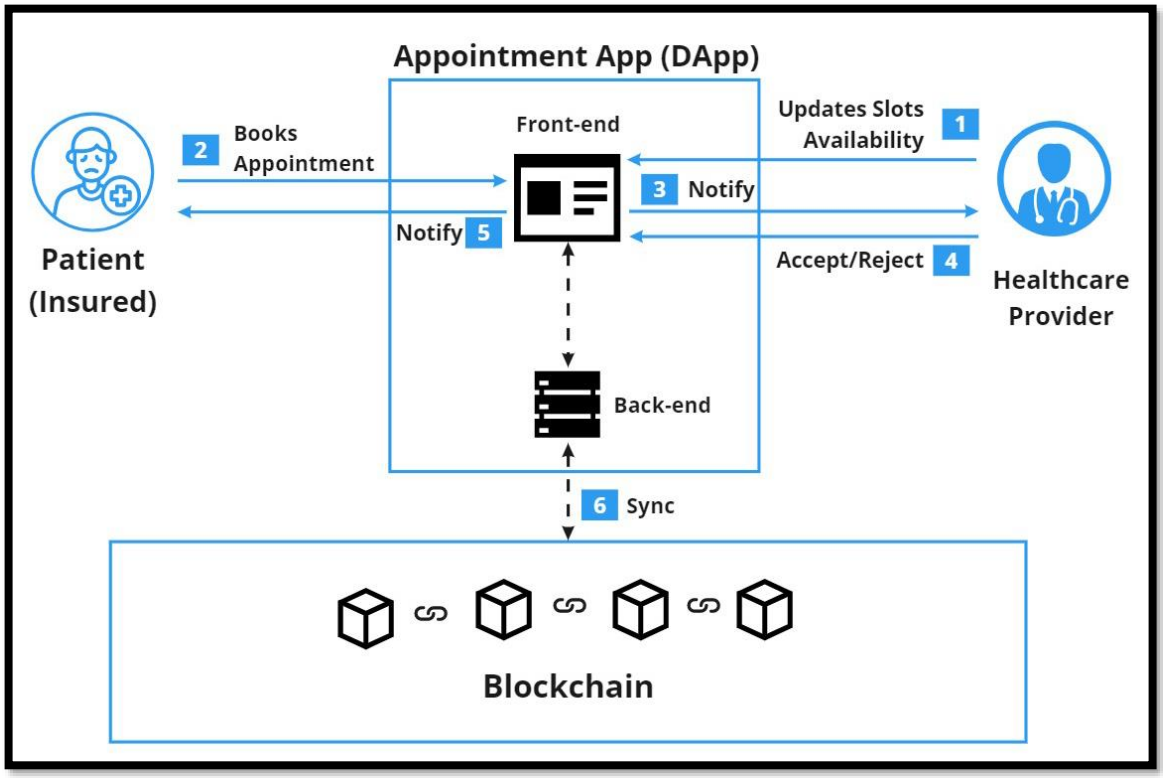
It is proposed that blockchain technologies are suitable as it is a tamper-proof and near-immutable audit database of the OHIP physician claims and transaction records.

At the same time, these claims and transactions can be viewed and decided upon in a distributed ledger by the health care provider, the Ministry, and patients to jointly validate claims and collaborate collaboratively to detect fraud and misuse.

The proposed framework aims to enable healthcare systems to do more proactive and transparent fraud detection rather than paying and investigating false OHIP claims.

Proposed Online Appointment System

Figure 15 Online Appointment System under OHIN



The proposed online appointment system through the Ministry-provided portal is the first point of access in OHIN, where the Healthcare providers update their slots availability. A

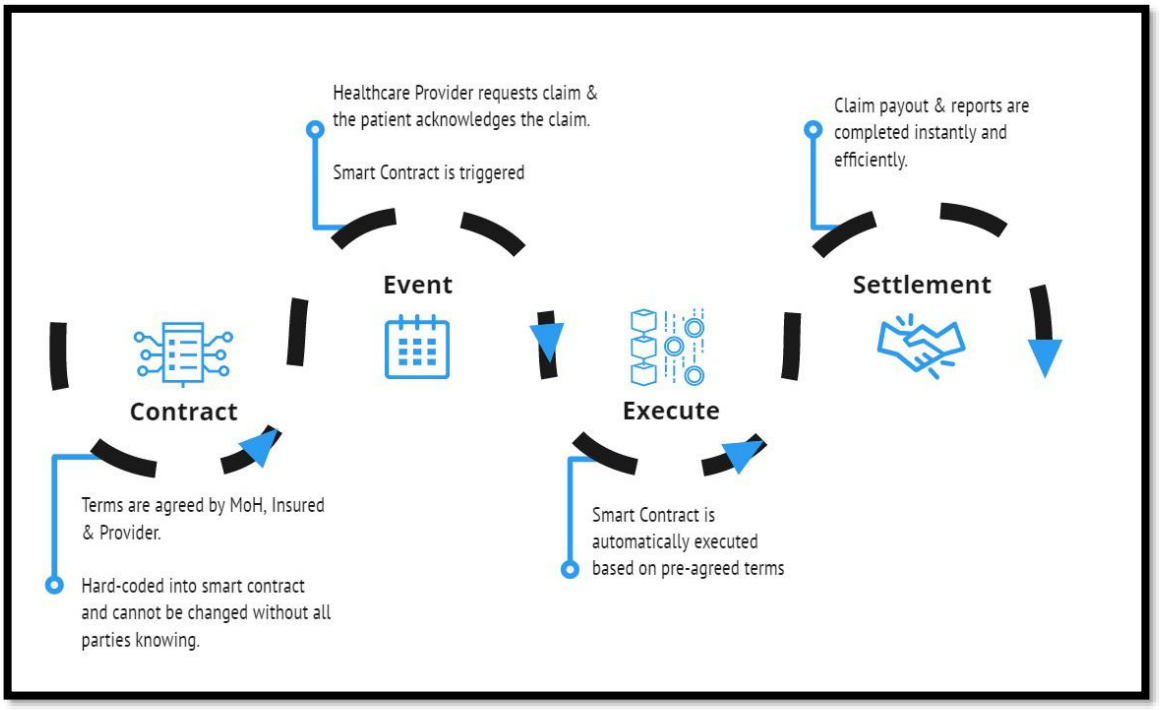
patient can view it and make an appointment accordingly directly through the application. The appointment process follows the following steps

1. The Healthcare provider updates the tentative slot availability to the application using the Front-end of the application, and the data is stored in the backend.
2. The patient checks the availability of slots and books an appointment by entering basic information and a briefing about the condition using the application's front-end. The data is stored in the backend.
3. The slot bookings are notified to the healthcare provider and reviewing and acknowledging the appointment.
4. The healthcare provider accepts the appointment or rejects it based on the actual availability.
5. The patient is notified with confirmation of his/her appointment.
6. Once the healthcare provider approves an appointment, the data is synchronized with the Blockchain. The information one’s synced to the Blockchain is immutable.

The appointment data is the first event in the medical claim process. The smart contract execution will not occur without an appointment by the patient, which will help prevent fake claims. The data stored on the Blockchain can be accessed by other access channels in the later stage of the claim process.

Proposed Smart Contract for OHIP physician claim processing

Figure 16 Smart Contract working under OHIN



A smart contract, a compilation of cryptographic code, contains pre-determined rules and instructions for completing a task. The criteria which are embedded in the code are met, the corresponding study or event is performed.[134]

Pre-defined Contract

A set of terms & conditions are agreed upon by all the parties involved, i.e., the healthcare provider, Ministry of Health, and the patients. In Fee-for-Service, the Schedule of Benefits as provided by the OMA forms the basis of a pre-defined contract. The smart contracts can

[134] What are Smart Contracts? - DCX Learn. (n.d.). Retrieved from https://dcxlearn.com/blockchain/smart-contract/ Accessed in April 2021

be embedded with the validation rules, which will use fraud analytics and help detect any fraudulent claims.

Events

An event triggers the execution of the contract. In OHIN, the events are booking an appointment by the insured (patient), submitting claim requests by the healthcare provider, and acknowledging the insured (patient).

Execute

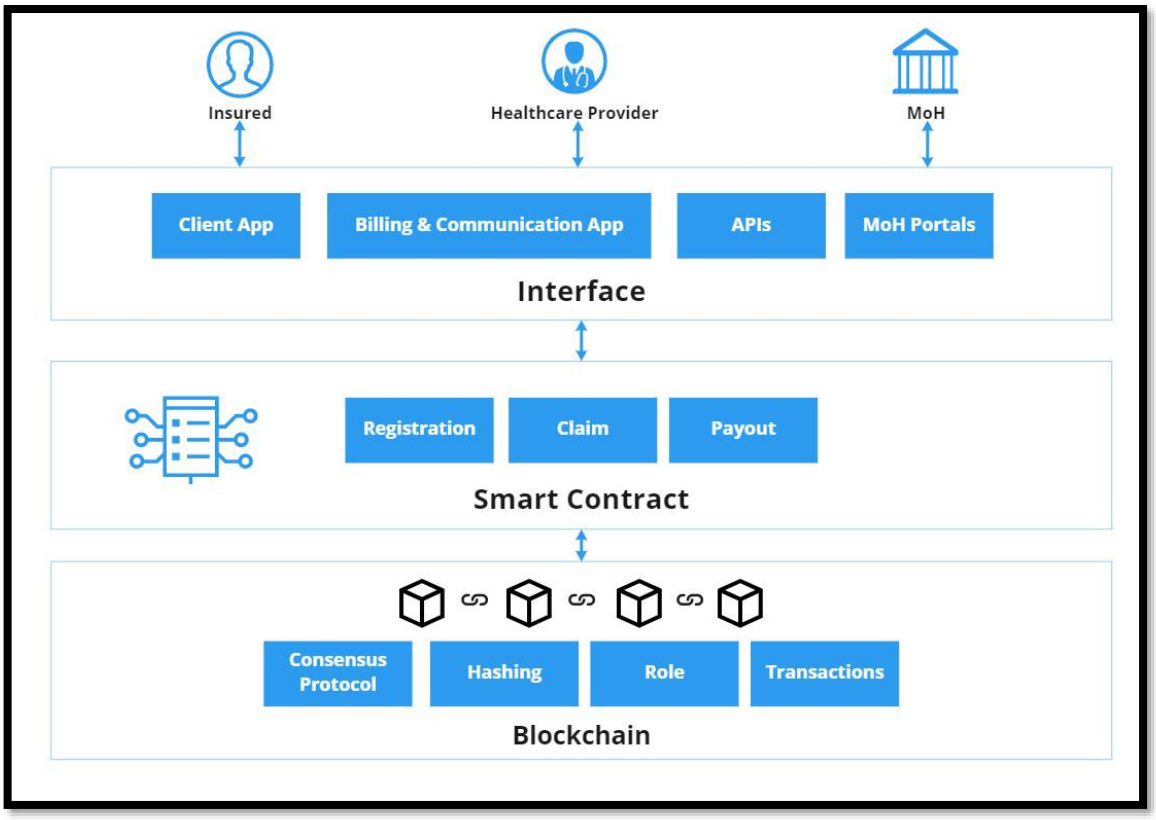
Based on all the external inputs received from the event, the smart contract is automatically executed based on the pre-agreed terms. In OHIN, once all the events are completed and acknowledged by the patient, the contract is executed.

Settlement

All the settlements are executed quickly and efficiently, i.e., the claim amount is disbursed to the healthcare provider. The claim report is sent to the healthcare provider and updated in the database.

OHIN System Design using Blockchain

Figure 17 Proposed System Design under OHIN using Blockchain Technology



The OHIN system consists of 3 significant entities

1) Insured (Resident)

2) Healthcare Provider

3) Ministry of Health (MoH)

The OHIN system has three layers

Interface

It is the primary layer where all the entities interact with the system.

Client App: The insured patient uses it to book an appointment, acknowledge the claim request, view drug prescriptions & lab reports, and access claim data & medical records.

Billing & Communication App: The healthcare provider uses it to submit the claim request and related files.

APIs: It is used to provide integrations to third-party providers to communicate with the OHIN network.

MoH Portal: The Ministry uses it to review and audit all the claims and disputes raised by the patients.

Smart Contract

It acts as an insurance policy to the insured and a contract to the healthcare provider. It checks the events triggered and processes the claims based on pre-defined terms.

Registration: The smart contract is deployed on the Blockchain when an eligible resident registers to the OHIN and when a healthcare provider joins the OHIN.

Claim: when an event occurs based on the data from the event, the claim process is executed.

Pay-out: Once the smart contract is executed, the pay-outs for the claim are disbursed by the contract.

Blockchain

Blockchain is a distributed database that allows multiple users to record and modify data. Because it only allows for the addition of data, it cannot be removed or changed once it has been entered.

Consensus Protocol: It is a mechanism of verifying data uploaded in Blockchain by reaching a decision among most participants and adding the block to the Blockchain once the consensus has reached.

There are various consensus protocols. The best-suited protocol for OHIN is the Proof of Authority consensus that gives a small and designated number of Blockchain stakeholders the power to validate transactions or interactions with the network and update its more or less distributed registry. The patients interact with the network while the OHIP agency from the Ministry has the power to validate the claims.

Hashing: Cryptographic hash functions generate a fixed-length character string from data records of any length. The hash of any transaction makes it easy to identify transactions on the Blockchain.

Role: Role-Based Access Control is a security need for software systems designed to be accessed by hundreds of users. It needs to determine who could add information to each block dynamically.

Transactions: All the activity in the OHIN is maintained as a transaction on the distributed ledger.

Privacy and security

Due to the sensitivity of dealing with personal healthcare information and the subsequent regulation for its protection, privacy and security are a concern. Personal Health Information Protection Act (PHIPA) is an Ontario provincial law that establishes essential guidelines for collecting, using, and distributing personal health information (PHI). PHI is defined as identifying information about a person in various forms relating to that person's physical or mental health or health services provided to that person. Patients have the right to access their health records and request corrections for any errors, along with the ability to restrict access to the medical history in part or whole under PHIPA.

Proposed Outcome of the Ontario Health Insurance Network

Cost-efficient to the Physicians.

The distributed ledger principle underpins blockchain technology, which removes the need for intermediaries. The third-party medical software provider charges approximately 2% of the paid claims per billing cycle billings to assist the physicians in the claim process. Any endorsed health care provider, patient, agencies can have access to the same pool of data modified in real-time when copies of the mutual ledger are stored across different users' locations. All transactions are authenticated and encrypted on a blockchain. All modifications to records are published as additions to the original data. Hence, it is cost-effective for the physicians as the claim process will be streamlined under OHIN.

Preventing fraud and exploitation

Cryptographic signatures and granular authorization settings are used to encrypt data stored on a blockchain-based ledger. It ensures that without sharing sensitive information, both parties can exchange data and check its authenticity. A shared, decentralized ledger allows to consolidate historical data and detect suspicious patterns using pre-defined validation rules based on industry standards to avoid the same claim being processed several times and manipulation of OHIP.

The proposed framework would also add a layer of aggregated data. It will enable tracking more systematic patterns of OHIP physician billing fraud, which can be mined for geographic locations, sensitive patient groups, and individual health care providers that may be vulnerable to these frauds.

Effective Machine learning is enabled from cryptographically authenticated multistakeholder claims data. (e.g., the claim submitted, validating the identity of stakeholders, and establishing consensus on the claim).With Blockchain, it will be possible to prevent frauds like overbilling, double billing, billings for services not rendered, misrepresentation of the time, date, place, and service, unbundling and upcoding. It could also help to detect trends and risk factors not likely from current static claims data.

Improvement in Transparency and Confidence

OHIP can be referred to as "walled gardens." Patients have very little access to information on how their physicians are billing the Ministry on their OHIP. They will not be able to quickly discover, for example, what services the physicians have billed on their health cards. There has been a demand for greater transparency in the payments made to

physicians. With the use of the proposed framework, there will be an enhancement in transparency and more accountability. Moreover, when the patients are made aware of how much is spent on their healthcare services, they will be more responsible and have improved confidence in the system. Furthermore, it will enhance the OHIP claim process's accountability and transparency

Claims administration made easier

It takes efforts to monitor each OHIP physician's claim and to remove inefficiency. The payment currently happens on an honour system. In a high-stakes environment, it is preferred to be adaptive to new technology and gain efficiency. Automating a significant portion of the OHIP fraud prevention system, time-consuming and repetitive processes like human claim analysis may be considerably reduced. As a result, integrating trust-based technology like blockchain into OHIP fraud prevention systems will have economic and technological advantages. Still, it would need to be tested further with real-world or simulated evidence to determine viability.

Blockchain technology and Smart Contracts can improve the management of claims and enable completion in a matter of minutes rather than months with blockchain. It will eliminate intermediaries, and automation will be able to take control of the entire claim process.

The claim process can be made even more efficient by utilizing Blockchain technology and Smart Contracts. There is lesser reason to doubt the claim's credibility once the patient has been involved in the process.

Audit trail

Smart contracts, which are gaining popularity in the property and casualty insurance industry, will simplify some procedures. A smart contract can initiate automated claim processing when combined with linked hardware when built-in sensors detect fraudulent claims or any erroneous submission, such as go off under pre-programmed conditions.

On the other hand, proper simplified insurance management necessitates increased confidence from healthcare providers and patients. The only way to achieve this equilibrium is to build a blockchain-based ecosystem with defined prominent participants. Under the proposed OHIN, when a new claim is added to the blockchain, distributed ledger technology helps verify the claim against the appointment initiated, visit verified, ensuring smooth claim administration.

Efficient process

The potential benefits of OHIN include the development of verified claims transaction logs and more efficient and validated workflows. First, rather than waiting for fraud to happen and only responding retrospectively, the mechanism would be configured to systematically monitor and deter possible fraud as well as other acts (such as overbilling, unintentional upcoding, and billing errors).

Using a layer of patients viewing the claim on a real-time basis is not presently available in the conventional OHIP claims adjudication processes.

Advantageous, especially after the advent of Bill 138

Bill 138 has accepted the stringent audit process, which is a concern to even the genuine doctors who practice with utmost integrity because of the time required in the compliance process. Implementing the proposed OHIN framework will enable sincere doctors to focus on their core competency of treating patients and the more monotonous task to be automated with the usage of Blockchain technology.

Role of a Forensic Accountant

Fraud prevention & detection

Forensic accountants are also actively engaged in fraud prevention. In a 2014 AICPA survey of international forensic accounting trends, the top services offered was Fraud prevention, detection, and response[135]which accounted for 44%.

Hence, A forensic accountant might be called in as a pre-emptive strike to manage fraud risk, just as a physician might recommend specific preventative health measures for patients. As a matter of right, forensic accountants can be used in a wide range of risk management engagements within businesses without the need for allegations. While working out the scope of a forensic accountant, there is no reason always to suspect fraud. Indica of Fraud can be detected by using Forensic accountant skills.

Whether health care providers are employed by the government or are privately owned, they can submit fraudulent bills or cost information in similar ways. The relationship should be considered by IFA to identify potential fraud schemes. For example, a government-employed physician paid a set salary has less incentive to bill for fictitious services than a private physician reimbursed based on the number of services provided, as in FFS. Fee-for-service payment has the disadvantage of encouraging providers to increase their compensation by performing extra and unnecessary services.

[135] The 2014 AICPA Survey on International Trends in Forensic and Valuation Services. Retrieved from https://aechile.cl/wp-content/uploads/2014/07/BIG-DATA2014-fvs-trend-survey-results-1.pdf Accessed in April 2021

Proactive Approach

A forensic accountant may take a proactive approach[136] (e.g., reviewing internal controls or identifying fraud exposure areas). Fraud prevention necessitates a set of policies and procedures that, when combined, reduce the likelihood of fraud while increasing the probability of detecting any fraudulent activity that may occur.

The possibility of being caught deters potential fraudsters. As a result, the existence of a comprehensive control system is critical to fraud prevention. Investing in fraud prevention should have a precise cost-benefit analysis. Preventing fraud is far more cost-effective than suffering preventable fraud and paying valuable resources on detecting, analyzing, charging, and cleaning up.

In the case of OHIP physician billing, the negative publicity that entire physicians are subjected to due to the actions of a few physicians can have a devastating effect on profession. A proactive fraud prevention mechanism can eliminate or reduce this impact.

Fraud Risk Assessment

The fraud risk assessment is critical for the development of effective anti-fraud programs and controls. Hence, the current OHIP physician billings and claim mechanism are critically evaluated. To effectively manage the fraud risks, Fraud risk assessment is a powerful proactive tool[137] is used in the fight against fraud in the OHIP physician billing process. The factors that affect the risk of OHIP physician billing fraud are as follows

[136] Forensic and Investigative Accounting (8th Edition), Chapter 1

[137] Fraud Examiner Manual: 2019 International Edition, ACFE, Fraud Risk Assessment Page 4.701

The nature of the work

Because of its very nature, OHIP physician fraudulent billing risks are an inherent risk. The Ministry must mitigate the inherent risk, and the residual risk must be significantly lower than the inherent risk.

The environment in which it operates

Medical practice is a self-regulatory profession. Furthermore, the majority of medical practitioners in Ontario are self-employed rather than government employees. As a result, having a standardized billing process that everyone can use is difficult.

Internal controls' effectiveness in the OHIP claim process.

With the right balance of preventive and detective controls, a sound internal control system can significantly reduce a company's fraud vulnerability. The detective controls, both manual and automated, in the OHIP post-physician billing review process is noticed, but these are designed to detect something wrong that has already happened. A well-designed and adequate internal control can deter the average fraudster by lowering the opportunity for fraud and raising the perception of detection.

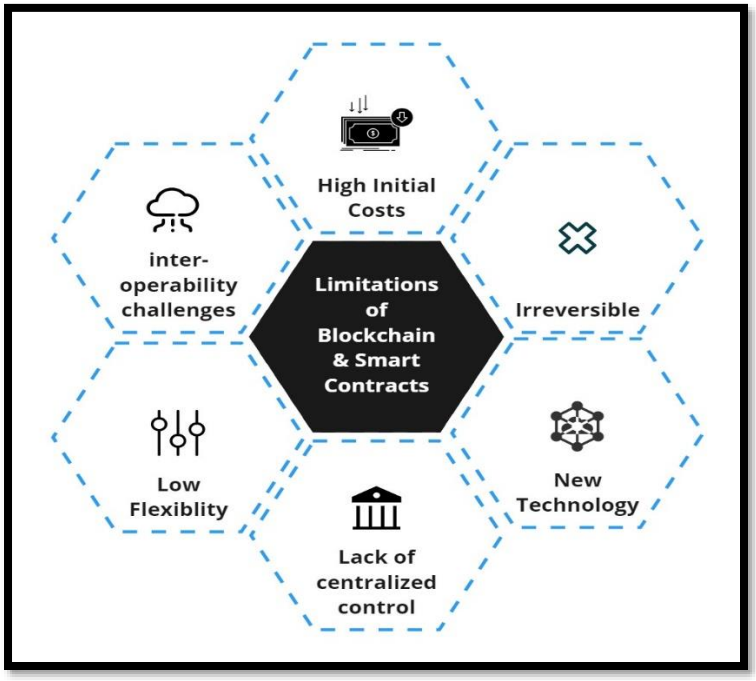
The Ministry's expected standards of ethics and values

Having a system made up of physicians whose ethics and values are entirely aligned with other ethics-oriented physicians is extremely difficult, if not impossible. Any significant discrepancies can raise the risk of OHIP physician billing fraud. Similarly, if the OHIP review mechanism shows consistency and predictability in handling and holding accountable unacceptable behavior, the risk of fraud is significantly reduced. To be consistent, a robust technology such as Blockchain and Smart Contracts will allow for smooth processing of legitimate claims while escalating fraudulent claims.

Limitations of Blockchain and Smart Contracts

This research paper has reviewed the advantages of blockchain and its benefits specific to the healthcare industry. However, as a recent technology, it also has certain limitations.

Figure 18 Limitations of Blockchain Technology and Smart Contracts



High Initial Cost

Although blockchain offers high cost and time savings, the high initial capital cost may be prohibitive. The high upfront costs of replacing equipment or upgrading technology constitute a significant impediment to adopting blockchain technology or other advanced concepts.[138] A network of nodes is required for distributed data sharing to build and maintain the blockchain in implementing Blockchain technology to Healthcare

[138] Hassan, N. U., Member, S., Yuen, C., & Niyato, D. (2019). Blockchain Technologies for Smart Energy Systems: Fundamentals, Challenges and Solutions. Retrieved from https://ieeexplore.ieee.org/document/8939186 Accessed in May 2021

Infrastructure, creating two issues. To begin, establishing such a healthcare network necessitates widespread support from the medical community. Existing medical systems maintain the status quo, and a new healthcare infrastructure may be too costly or difficult to implement on a large scale. Second, maintaining a blockchain network necessitates a significant amount of computing power, increasing hardware costs and increasing the amount of energy consumed by a hospital system.[139]

Irreversible

Users verify transactions in the blockchain using certificate authentication, cryptocurrencies, and other methods. Even if both parties mutually agree, the transactions cannot be reversed. There is no way to undo a contract once it has been executed.

New Technology

Institutions must abandon their current networks and begin to build new ones to implement Blockchain. Integration is a complex process, and most institutions do not want to integrate Blockchain into their existing systems. For all stakeholders, the technical complexity of the cryptography and networking involved can be challenging to comprehend. Due to the complexity of blockchain setup, many patients may be hesitant to view and manage the claim processing.[140]

[139] Yaeger, K., Martini, M., Rasouli, J., & Costa, A. (2019). Emerging Blockchain Technology Solutions for Modern Healthcare Infrastructure. Journal of Scientific Innovation in Medicine, 2(1), 1. https://doi.org/10.29024/jsim.7 Accessed in May 2021

[140] Alla, S., Soltanisehat, L., Tatar, U., & Keskin, O. (2018). Blockchain Technology in Electronic Healthcare System Curriculum Development- https://www.researchgate.net/publication/325542378 Accessed in May 2021

Lack of centralized control

In a distributed database like blockchain, extra effort must be put in to ensure that all nodes in the network agree. Depending on the consensus mechanism in use, this could entail a lot of back-and-forth communication and deal with forks and rollbacks. While centralized databases must deal with conflicting and aborted transactions, these are far less common when transactions are queued and processed in one place.

Low flexibility

One of the disadvantages of blockchain is its difficulty in understanding the average person. Blockchain technology has complex concepts and processes that have yet to be refined to the point where the average person can easily digest and consume information on how to use it, so it is not yet ready for widespread adoption.

Interoperability Challenges

Despite the many ways blockchain could enable patient-led interoperability, there are a few roadblocks to overcome. The first impediment is the sheer volume and size of clinical data. Clinical data is built on high-volume, high-frequency transactions, and the size of clinical information is growing thanks to modern technological advancements exponentially. With current technology, it is impossible to store this data on-chain due to the distributed nature of a blockchain. Furthermore, on blockchains based on proof of work, new transaction verification can take time (such as the Bitcoin). These constraints favor small-scale, infrequent transactions.

Potential Limitations and Challenges of OHIN

However, there are some drawbacks and barriers in implementing the proposed OHIN framework. To implement OHIN, complete cooperation from all parties in the OHIP claims lifecycle, such as the Ministry of Health and its agencies, OMA, the health care practitioner, and finally, the patients, are crucial.

It necessitates a thorough integration with current information management programs, identifying interoperability issues, and ensuring relevant data specifications.

Integrating healthcare provider billing and sales management period processes, current databases and APIs, and a front end that will communicate with patients, on the other hand, would almost certainly be challenging.

The possibility of the abuse of the framework structure is to be considered, and it must therefore be mitigated. For example, there may be an effort to sway the consensus of all parties on a recorded claim. It covers scenarios under which the patient is a co-conspirator of a fraud (Collusion between Patient and the Health care provider) and exploitation operation and methods in which patient validation leads to the erroneous adjudication of a fraudulent claim. It is a particular concern when a patient has a solid motive to engage in and benefit from fraud and abuse.

With changes to the smart contract claims adjudication procedure and consent structure unique to high-risk claims and patient profiles, the OHIN framework will recognize and proactively avoid situations where both the provider and the patient engage in fraud and abuse.

The OHIN framework is based on a growing body of work that seeks to use blockchain technologies to transform healthcare data and claims workflows. Many of these plans face acceptance and development challenges that will necessitate further experimentation, evaluation, and constructive cooperation with the healthcare sector.

Blockchain is a long-term investment that reinvents processes to increase efficiency while lowering costs and increasing value for everyone involved, from providers to consumers. However, the Ministry of Health requires a lot of support and coordination from the OMA and physicians to achieve this larger goal. Though there are several components to determining feasibility, such as cost-benefit analysis and infrastructure suitability, one crucial element is educating laypeople about the OHIN and its role in the process.

However, while transparency is essential, it can increase uncertainty and outweigh its benefits if proper education, awareness, and relevant disclosures are not presented.

Scope for future research.

The OHIN framework may further be expanded to include lab test results, Drug and Pharmacy Service Information, clinical and diagnostic imaging to have an end-to-end information availability for the patients and ease as access. This advantage of viewing all this patient-focused data is now available for the health care providers only.

Our research covered only FFS under OHIP physician billing as its transaction specific. Still, the framework could be further tested to extend to Ontario Drug Benefit Program, OHIP+, and Trillium Drug Program, which has similar challenges as OHIP. The advantages in these would be entire scheme could be covered as all these are reimbursed on actual events and do not include a flat fee.

CONCLUSION

The current OHIP physician claim process is evaluated within the current healthcare environment in Ontario. Like any other insurance plan, it is observed that OHIP requires investigation and oversight, provided by the new Bill 138, which will result in adequate detection controls in OHIP physician billing.

As noted in the 2016 Audit General Report, the need for enhanced detection controls arose from a lack of enforcement, consequences for wrongdoing, actions for fraud, and a lack of infrastructure to deter fraudulent claims. The same was reaffirmed in the Auditor General's 2018 Follow-up Report.

For deriving the scope for improved transparency in the OHIP physician billing, reliance is placed that transparency in any process improves the efficiency of that process and reduces the area for fraud. As desired by all, transparency in OHIP physician billing will also benefit all core participants, including physicians, OMA, the Ministry of Health, and patients.

This framework focuses on preventive controls in the proposed framework, which will make it less likely for a healthcare provider to commit fraud. It's more psychological than the fact that an OHIP physician claim is out there for a patient to review. The fear that one of those patients will be technologically savvy enough to uncover any fraudulent billing scheme will deter any such activity. And operating in a transparent environment will pose no risk to the majority of physicians who are completely honest and provide service with integrity.

Ontario Health Insurance Network (OHIN) is proposed to facilitate transparency in the physicians' OHIP billings. While blockchain isn't the end-all solution, it can help with several issues in the healthcare industry, including data security, interoperability, and data accessibility[141].

Finally, blockchain for healthcare significantly reduces the current healthcare landscape's inefficiency and waste. Conventionally, Health insurers end up paying claims first and then identifying inaccurate payments and reconciling overpayments and underpayments. Blockchain can help because it provides transparency to all parties by allowing payers and providers to negotiate claims because of its shared ledger capabilities. Blockchain can provide solutions for both the billing and claim processes. If the billing process is linked to the blockchain, there is no way for a health care provider to overcharge a patient or add a service that the patient never requested in the first place. It will deter fraud and increase the transparency in OHIP Physician Billings.

[141] Digital Disruption: The Transformation of Blockchain in Healthcare. Retrieved from https://healthcareweekly.com/digital-disruption-blockchain-in-healthcare/ Accessed in May 2021

Bibliography

‘That’s an injection mill.’ Ontario’s top-billing pain doctors capitalize on the province’s lax rules, running up the public’s tab for chronic pain management | The Star. (n.d.). Retrieved from https://www.thestar.com/news/investigations/2020/09/28/thats-an-injection-mill-ontarios-top-billing-pain-doctors-capitalize-on-provinces-lax-rules-running-up-the-publics-tab-for-chronic-pain-management.html

“I AM ACCOUNTABLE”: Chatham doctor who repaid OHIP $31Gs handed suspension | Toronto Sun. (n.d.). Retrieved from https://torontosun.com/news/provincial/i-am-accountable-chatham-doctor-who-repaid-ohip-31gs-handed-suspension

Ten popular health care provider fraud schemes. (n.d.). Retrieved from https://www.acfe.com/article.aspx?id=4294976280

15 Top Blockchain in Healthcare Examples Helping Revive the Industry 2021 | Built In. Retrieved from https://builtin.com/blockchain/blockchain-healthcare-applications-companies

2019 Ontario Budget | Chapter 3. (n.d.). Retrieved from https://budget.ontario.ca/2019/chapter-3.html#t3-13

A platform approach in solution business: How platform openness can be used to control solution networks - ScienceDirect. (n.d.). Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0019850118303432

Accessing Your EHR | eHealth Ontario | It’s Working for You. (n.d.). Retrieved from https://ehealthontario.on.ca/en/patients-and-families/accessing-your-ehr

Ahmadisheykhsarmast, S. (2018). Smart Contracts in Construction Industry. https://www.researchgate.net/publication/329363162

Alla, S., Soltanisehat, L., Tatar, U., & Keskin, O. (2018). Blockchain Technology in Electronic Healthcare System Curriculum Development https://www.researchgate.net/publication/325542378

Allam, Z. (2018). ON SMART CONTRACTS AND ORGANISATIONAL PERFORMANCE: A REVIEW OF SMART CONTRACTS THROUGH THE BLOCKCHAIN TECHNOLOGY. 11(2), 137–156. https://doi.org/10.1515/rebs-2018-0078

Architecture Explained — hyperledger-fabric docs master documentation. (n.d.). Retrieved from https://hyperledger-fabric.readthedocs.io/en/release-1.3/arch-deep-dive.html

As per IBC: We're fighting 'prolific fraud' in Canada | Insurance Business. (n.d.). Retrieved from https://www.insurancebusinessmag.com/ca/news/healthcare/ibc-were-fighting-prolific-fraud-in-canada-162456.aspx

Attallah (Re), [2020] OCPSD No 38, 2020 ONCPSD 38

Bill 138, Schedule 15 Summary of Amendments Before and After-Impact on Physicians ORIGINAL BILL AMENDED Direct Recovery by OHIP Without a formal hearing. (n.d.) Retrieved from https://content.oma.org/wp-content/wp-private.php?filename=Bill-138-Amendments-Summary-2019-Final.pdf

Blockchain For Healthcare: Use Cases And Applications | 101 Blockchains. Retrieved from https://101blockchains.com/blockchain-for-healthcare/

Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability - ScienceDirect. (n.d.). Retrieved from https://www.sciencedirect.com/science/article/pii/S200103701830028X?via%3Dihub

Bob Bell Contributor. (2019). Increased oversight of OHIP is overdue. Toronto Star. https://www.thestar.com/opinion/contributors/2019/11/05/increased-oversight-of-ohip-is-overdue.html

Bulletin, The Physician Payment Review Board, becomes Functional. Retrieved from https://www.health.gov.on.ca/en/pro/programs/ohip/bulletins/4000/bul4511.pdf

Canada | Commonwealth Fund. (n.d.). Retrieved from https://www.commonwealthfund.org/international-health-policy-center/countries/canada

Canada Health Act Annual Report 2019-2020, Retrieved from https://www.canada.ca/en/health-canada/services/publications/health-system-services/canada-health-act-annual-report-2019-2020.html

Canada's Health Care System - Canada.ca. (n.d.). Retrieved from https://www.canada.ca/en/health-canada/services/health-care-system/reports-publications/health-care-system/canada.html

Canadian Institute for Health Information. (2017). Unnecessary Care in Canada. www.cihi.cacopyright@cihi.caISBN978-1-77109-569-3

Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2018). Blockchain-Based Medical Records Secure Storage and Medical Service Framework. Journal of Medical Systems, 43(1), 1–9. https://doi.org/10.1007/s10916-018-1121-4

Classification and main characteristics of blockchain networks. | Download Table. (n.d.). Retrieved from https://www.researchgate.net/figure/Classification-and-main-characteristics-of-blockchain-networks_tbl1_329136952

CMPA - About the CMPA. (n.d.). Retrieved from https://www.cmpa-acpm.ca/en/about

Commitment to the Future of Medicare Act, 2004, S.O. 2004, c. 5. (n.d.). Retrieved from https://www.ontario.ca/laws/statute/04c05

CPSO - Doctor Details. (n.d.). Retrieved from https://doctors.cpso.on.ca/DoctorDetails/Gabriel---Nicola-Attallah/0189886-77343

Data Protection: Data In transit vs. Data At Rest | Digital Guardian. (n.d.). Retrieved from https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest

Demestichas, K., Peppes, N., Alexakis, T., & Adamopoulou, E. (2020). Blockchain in agriculture traceability systems: A review. Applied Sciences (Switzerland), 10(12), 1–22. https://doi.org/10.3390/APP10124113

Digital Disruption: The Transformation of Blockchain in Healthcare. Retrieved from https://healthcareweekly.com/digital-disruption-blockchain-in-healthcare/

Distributed Ledgers Definition. (n.d.). Retrieved from https://www.investopedia.com/terms/d/distributed-ledgers.asp

eHealth Ontario | It's Working For You. (n.d.). Retrieved from https://ehealthontario.on.ca/en/health-care-professionals/digital-health-services

eHealth Services (eHS) Info. (n.d.). Retrieved May 27, 2021, from https://www.ehealthontario.ca/wps/portal/eHealthPortal/Applications/EhsInfo/

Engelhardt, M. A. (2017). Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. Technology Innovation Management Review, 7(10), 22–34. https://doi.org/10.22215/timreview/1111

Etobicoke doctor charged with defrauding OHIP: Longwoods.com. (n.d.). Retrieved from https://www.longwoods.com/newsdetail/8239

Expenditure Estimates 2019-20: Ministry of Health and Long-Term Care. (n.d.). Retrieved from https://www.fao-on.org/en/Blog/Publications/estimates-health-2019

Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. Journal of Medical Systems, 42(8). https://doi.org/10.1007/s10916-018-0993-7

Fee-for-service: an ethical conflict | Impact Ethics Retrieved from https://impactethics.ca/2017/02/22/fee-for-service-an-ethical-conflict/

Fighting Fraud, Waste, and Abuse for a Healthy Business retrieved from https://www.claimsecure.com/en/whats-new-blog/2019/march/11/fighting-fraud-waste-and-abuse-for-a-healthy-business/

Forensic and Investigative Accounting (8th Edition)

Fraud Examiner Manual: 2019 International Edition, ACFE, Fraud Risk Assessment Page 4.701

Fraud risk formulas for financial statement audits. (n.d.). Retrieved from https://www.researchgate.net/publication/228804816_Fraud_risk_formulas_for_financial_statement_audits

Freedom of Information and Protection of Privacy Manual: Chapter 1: The Legislation | Ontario.ca. (n.d.). Retrieved from https://www.ontario.ca/document/freedom-information-and-protection-privacy-manual/chapter-1-legislation

Gilcrest, J., & Carvalho, A. (n.d.). Smart Contracts: Legal Considerations. Retrieved from http://coinmarketcap.com

Góngora Alonso, S., Arambarri Basañez, J., Lopez-Coronado, M., Arambarri, J., López-Coronado, M., & de la Torre Díez, I. (2019). Proposing New Blockchain Challenges in eHealth Data mining in Mental Health View project IN LIFE Project View project Proposing New Blockchain Challenges in eHealth. Article in Journal of Medical Systems. https://doi.org/10.1007/s10916-019-1195-7

Government to phase out red and white OHIP cards | AFHTO. (n.d.). Retrieved from https://www.afhto.ca/news-events/news/government-phase-out-red-and-white-ohip-cards

Hartel, P., & Mark Van Staalduinen, |. (n.d.). ARTICLE TYPE Truffle tests for free-Replaying Ethereum smart contracts for transparency. Retrieved from http://truffleframework.com

Hassan, N. U., Member, S., Yuen, C., & Niyato, D. (2019). Blockchain Technologies for Smart Energy Systems: Fundamentals, Challenges and Solutions. Retrieved from https://ieeexplore.ieee.org/document/8939186

Health Insurance Act, R.S.O. 1990, c. H.6. (n.d.). Retrieved from https://www.ontario.ca/laws/statute/90h06

Health Services Appeal and Review Board - Public Appointments Secretariat. (n.d.). Retrieved from https://www.pas.gov.on.ca/Home/Agency/294

Health spending | CIHI. (n.d.). Retrieved from https://www.cihi.ca/en/health-spending

Hepburn, B. (n.d.). Why can't patients see our OHIP billings? Toronto Star; Toronto Star. Retrieved May 6, 2021, from https://www.thestar.com/opinion/star-columnists/2019/07/10/why-cant-patients-see-our-ohip-billings.html

https://www.health.gov.on.ca/en/pro/programs/ohip/docs/physician_FFS_post_pay_audit_process.pdf

Hylock, R. H., & Zeng, X. (2019). A blockchain framework for patient-centered health records and exchange (healthChain): Evaluation and proof-of-concept study. Journal of Medical Internet Research, 21(8), e13592. https://doi.org/10.2196/13592

Individual Personal Health Information (PHI) Access Requests - Ontario Health Insurance Plan - Ministry Programs - Public Information - MOHLTC. (n.d.). Retrieved from https://www.health.gov.on.ca/en/public/programs/ohip/phi_access/default.aspx

Jiang, T., Fang, H., & Wang, H. (2019). Blockchain-based internet of vehicles: Distributed network architecture and performance analysis. IEEE Internet of Things Journal, 6(3), 4640–4649. https://doi.org/10.1109/JIOT.2018.2874398

Justice Department Recovers Over $3 Billion from False Claims Act Cases in the Fiscal Year 2019 | OPA | Department of Justice. (n.d.). Retrieved from https://www.justice.gov/opa/pr/justice-department-recovers-over-3-billion-false-claims-act-cases-fiscal-year-2019

Kamel Boulos, M. N., Wilson, J. T., & Clauson, K. A. (2018). Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare. In International Journal of Health Geographics (Vol. 17, Issue 1, p. 25). BioMed Central Ltd. https://doi.org/10.1186/s12942-018-0144-x

Kelly, P., & Hartley, C. A. (2010). Casino gambling and workplace fraud: a cautionary tale for managers. Management Research Review, 33(3), 224–239. https://doi.org/10.1108/01409171011030381

Kenyon, W. and Tilton, P. D. (2006). Potential Red Flags and Fraud Detection Techniques - A Guide to Forensic Accounting Investigation - Wiley Online Library. (n.d.). Retrieved from https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119200048.ch13

Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. Applied Sciences (Switzerland), 9(9), 1736. https://doi.org/10.3390/app9091736

Kshetri, N. K. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 41(10), 1027–1038. https://doi.org/10.1016/j.telpol.2017.09.003

Lyttle v Ontario (Health Insurance Plan, General Manager), [2004] OJ No 4575, 134 ACWS (3d) 1103

Mackey, T. K., Kuo, T. T., Gummadi, B., Clauson, K. A., Church, G., Grishin, D., Obbad, K., Barkovich, R., & Palombini, M. (2019). "Fit-for-purpose?" - Challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Medicine, 17(1), 1–17. https://doi.org/10.1186/s12916-019-1296-7

Madumidha, S., Ranjani, P. S., Varsinee, S. S., & Sundari, P. S. (2019). Transparency and traceability: In food supply chain system using blockchain technology with internet of things. Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI 2019, 983–987. https://doi.org/10.1109/ICOEI.2019.8862726

Major federal transfers - Canada.ca Retrieved from https://www.canada.ca/en/department-finance/programs/federal-transfers/major-federal-transfers.html#Ontario

MANDEL: "Incompetent" Mississauga doc overbilled OHIP $146,000 | Toronto Sun. (n.d.). Retrieved from https://torontosun.com/news/local-news/mandel-incompetent-mississauga-doc-overbilled-ohip-146000

Mansor, N., & Abdullahi, R.' U. (2015). Understanding the Convergent and Divergent for Future Research Article in International Journal of Academic Research in Accounting Finance and Management Sciences · October. https://doi.org/10.6007/IJARAFMS/v5-i4/1823

Miller, A. (2013). Medical fraud north of the 49th. In CMAJ: Canadian Medical Association journal = journal de l'Association medicale canadienne (Vol. 185, Issue 1). https://doi.org/10.1503/cmaj.109-4358

Ministry of Health (Ontario) - Wikipedia. (n.d.). Retrieved from https://en.wikipedia.org/wiki/Ministry_of_Health_(Ontario)

Ministry of Health and Long-Term care. (2016). Technical Specification for Medical Claims Electronic Data Transfer (MCEDT) Service via Electronic Business Services (EBS) (p. 35). Ministry of Health and Long-Term Care. http://www.health.gov.on.ca/en/pro/publications/ohip/docs/techspec_mcedt_ebs.pdf

Ministry of Health and Long-Term Care. (2017). Resource Manual for Physicians. https://www.health.gov.on.ca/en/pro/publications/ohip/docs/resource_manual_for_Physicians.pdf

Ministry of Health and Long-Term care. (2018). Medical Claims Electronic Data Transfer (MC EDT) Reference Manual. https://www.health.gov.on.ca/en/pro/publications/ohip/docs/mc_edt_reference_manual.pdf

Ministry of Health, (2021). Summary of Physician FFS Post-Payment Audit Process Retrieved from https://www.health.gov.on.ca/en/pro/programs/ohip/docs/physician_FFS_post_pay_audit_process_summary.pdf

Ministry of Health, OHIP Division, (n.d.). The physician fee-for-service post-payment audit process. Retrieved from https://www.health.gov.on.ca/en/pro/programs/ohip/docs/physician_FFS_post_pay_audit_process.pdf

MOHLTC - Resource Manual for Physicians - Section 2 - Physician Payment and Policy - 2.2. (n.d.). Retrieved from https://www.health.gov.on.ca/english/providers/pub/ohip/physmanual/pm_sec_2/2-2.html

National Health Expenditure Trends | CIHI. (n.d.). Retrieved from https://www.cihi.ca/en/national-health-expenditure-trends

Niagara eye doctor charged with fraud | wellandtribune.ca. (n.d.). Retrieved from https://www.wellandtribune.ca/news/niagara-region/2019/07/11/niagara-eye-doctor-charged-with-fraud.html?rf

Nugent, T., Upton, D., & Cimpoesu, M. (2016). Open Peer Review Improving data transparency in clinical trials using blockchain smart contracts [version 1; peer review: 3 approved]. https://doi.org/10.12688/f1000research.9756.1

Office of the Auditor General of Ontario. (2016). Annual Report 2016. (Pages 551 to 603) https://www.auditor.on.ca/en/content/annualreports/arreports/en16/2016AR_v1_en_web.pdf

OHIP Fraud - Ontario Health Insurance (OHIP) - Publications - Public Information - MOHLTC. (n.d.). Retrieved from https://www.health.gov.on.ca/en/public/publications/ohip/card_fraud.aspx

On Availability for Blockchain-Based Systems. (n.d.). Retrieved from https://www.researchgate.net/publication/320651459_On_Availability_for_Blockchain-Based_Systems

On June 20, 2019, the Ministry of Health and Long-Term Care was split into the Ministry of Health and the Ministry of Long-Term Care.

One of Ontario's top-billing doctors faces discipline for alleged 'incompetent' care and inappropriate billings | The Star. (n.d.). Retrieved from https://www.thestar.com/news/investigations/2019/08/22/one-of-ontarios-top-billing-doctors-faces-discipline-for-alleged-incompetent-care-and-inappropriate-billings.html

Ontario auditor's report highlights doctors' billing, casino concerns | Toronto Sun. (n.d.). Retrieved from https://torontosun.com/news/provincial/ontario-auditor-general-to-release-annual-report

Ontario Doctors Call for Changes to Proposed Audit System. (n.d.). Retrieved from https://www.newswire.ca/news-releases/ontario-doctors-call-for-changes-to-proposed-audit-system-895166275.html

Ontario Health Insurance Plan - Wikipedia. (n.d.). Retrieved from https://en.wikipedia.org/wiki/Ontario_Health_Insurance_Plan

Ontario Health Insurance Plan INFO Bulletin. New Physician Post-Payment Review Process. (2021). https://www.health.gov.on.ca/en/pro/programs/ohip/bulletins/redux/bul210309.aspx

Ontario Ministry of Health and Long-Term Care - Health Care Providers - Declaration of PHIPA as substantially similar to PIPEDA - Q&A. (n.d.). Retrieved from https://www.health.gov.on.ca/english/providers/project/priv_legislation/phipa_pipeda_qa.html

Ontario pain doctor billings 'shocking,' Doug Ford says after Star revelations | The Star. (n.d.). Retrieved from https://www.thestar.com/news/investigations/2020/09/28/ontario-pain-doctor-billings-shocking-doug-ford-says-after-star-revelations.html

OPP charge Whitby doctor for fraudulent OHIP billings totalling $170K | CTV News. (n.d.). Retrieved from https://northernontario.ctvnews.ca/opp-charge-whitby-doctor-for-fraudulent-ohip-billings-totalling-170k-1.5176508

Oversight system for doctors' OHIP billings slammed as 'ineffective' - WWWHive. (n.d.). Retrieved from https://wwwhive.com/2019/07/01/oversight-system-for-doctors-ohip-billings-slammed-as-ineffective/

Pace, G. J., Ellul, J., & Azzopardi, S. (2018). Monitoring Smart Contracts: ContractLarva and Open Challenges Beyond. https://www.researchgate.net/publication/327834131

Plan to Build Ontario Together Act, 2019, S.O. 2019, c. 15 - Bill 138. (n.d.). Retrieved from https://www.ontario.ca/laws/statute/s19015#BK17

Primary Care Payment Models in Ontario - Health Care Professionals - MOHLTC. (n.d.). Retrieved from https://www.health.gov.on.ca/en/pro/programs/pcpm/

Proposed Changes to OHIP include Fundamentally Flawed Policies. (n.d.). Retrieved from https://www.newswire.ca/news-releases/proposed-changes-to-ohip-include-fundamentally-flawed-policies-815834078.html

Recommendations to protect patients and health care practices from Medicare and Medicaid fraud. (n.d.). Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7323645/

Section 2 of the Canada Health Act. (n.d.). Retrieved from https://laws-lois.justice.gc.ca/eng/acts/c-6/fulltext.html

Security Risks & Concerns for Blockchain Cryptocurrencies. (n.d.). Retrieved from https://www.businessinsider.com/cryptocurrency-blockchain-security?IR=T

Specialty CANADA NL PEI NS NB QC ON MB SK AB BC TERR Laboratory Medicine Specialists. (n.d.). Retrieved from https://www.cma.ca/sites/default/files/2019-11/2019-01-spec-prov_1.pdf

Star Editorial Board. (2019a). Time to reveal individual MD's OHIP billings. Toronto Star. https://www.thestar.com/opinion/editorials/2019/04/14/time-to-reveal-individual-mds-ohip-billings.html

Star Editorial Board. (2019b). Transparency on what doctor's bill OHIP informs the health-care debate. Toronto Star. https://www.thestar.com/opinion/editorials/2019/06/27/transparency-on-what-doctors-bill-ohip-informs-the-health-care-debate.html

Summary report. Physicians in Canada, 2019, Canadian Institute of Health Information, Page 33 Retrieved from https://secure.cihi.ca/free_products/physicians-in-Canada-report-en.pdf

The 2014 AICPA Survey on International Trends in Forensic and Valuation Services. Retrieved from https://aechile.cl/wp-content/uploads/2014/07/BIG-DATA2014-fvs-trend-survey-results-1.pdf

The Canadian Health Care System Retrieved fromhttps://www.loc.gov/law/help/medical-malpractice-liability/canada.php

They're Ontario's top-billing doctors, but for years their identities have been kept secret. Until now - WWWHive. (n.d.). Retrieved from https://wwwhive.com/2019/06/27/theyre-ontarios-top-billing-doctors-but-for-years-their-identities-have-been-kept-secret-until-now/

Thornton, D., Brinkhuis, M., Amrit, C., & Aly, R. (2015). Categorizing and Describing the Types of Fraud in Healthcare. Procedia Computer Science, 64, 713–720. https://doi.org/10.1016/j.procs.2015.08.594

Unnecessary Care in Canada: CIHI and CWC Joint Report Released - Choosing Wisely Canada. (n.d.). Retrieved from https://choosingwiselycanada.org/perspective/unnecessary-care-canada-cihi-cwc-joint-report-released/

Value-for-Money Audit: Virtual Care: Use of Communication Technologies for Patient Care (2020). Retrieved from https://www.auditor.on.ca/en/content/annualreports/arreports/en20/20VFM_08virtualcare.pdf

Weber, I., Gramoli, V., Ponomarev, A., Staples, M., Holz, R., Tran, A. B., & Rimba, P. (2017). On availability for blockchain-based systems. Proceedings of the IEEE Symposium on Reliable Distributed Systems, 2017-Septe, 64–73. https://doi.org/10.1109/SRDS.2017.15

What are Smart Contracts? - DCX Learn. (n.d.). Retrieved from https://dcxlearn.com/blockchain/smart-contract/

What is Blockchain Security | IBM. (n.d.). Retrieved from https://www.ibm.com/topics/blockchain-security

What is Digital Certificate? | Definition of Digital SSL Certificates. (n.d.). Retrieved from https://www.comodo.com/resources/small-business/digital-certificates.php

What is SSL, TLS? And how this encryption protocol works | CSO Online. (n.d.). Retrieved from https://www.csoonline.com/article/3246212/what-is-ssl-tls-and-how-this-encryption-protocol-works.html

Why the Blockchain is So Secure - open source for you. (n.d.). Retrieved from https://www.opensourceforu.com/2019/05/why-the-blockchain-is-so-secure/

Wilson, A. (2004). Employee Dishonesty: National Survey of Risk Managers on Crime. In Journal of Economic Crime Management Winter (Vol. 2, Issue1. https://www.utica.edu/academic/institutes/ecii/publications/articles/BA2D546B-BC9E-1844-8B0ADF5FB1B84B99.pdf

Wolfe, D. T., & Hermanson, D. R. (2004). The Fraud Diamond: Considering the Four Elements of Fraud. https://digitalcommons.kennesaw.edu/facpubs

Yaeger, K., Martini, M., Rasouli, J., & Costa, A. (2019). Emerging Blockchain Technology Solutions for Modern Healthcare Infrastructure. Journal of Scientific Innovation in Medicine, 2(1), 1. https://doi.org/10.29024/jsim.7

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on Blockchain technology? - A systematic review. PLoS ONE, 11(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

Young, C. R. (n.d.). A Lawyer's Divorce: Will Decentralized Ledgers and Smart Contracts Succeed In Cutting Out the Middleman? (Vol. 96). Retrieved from https://openscholarship.wustl.edu/law_lawreview

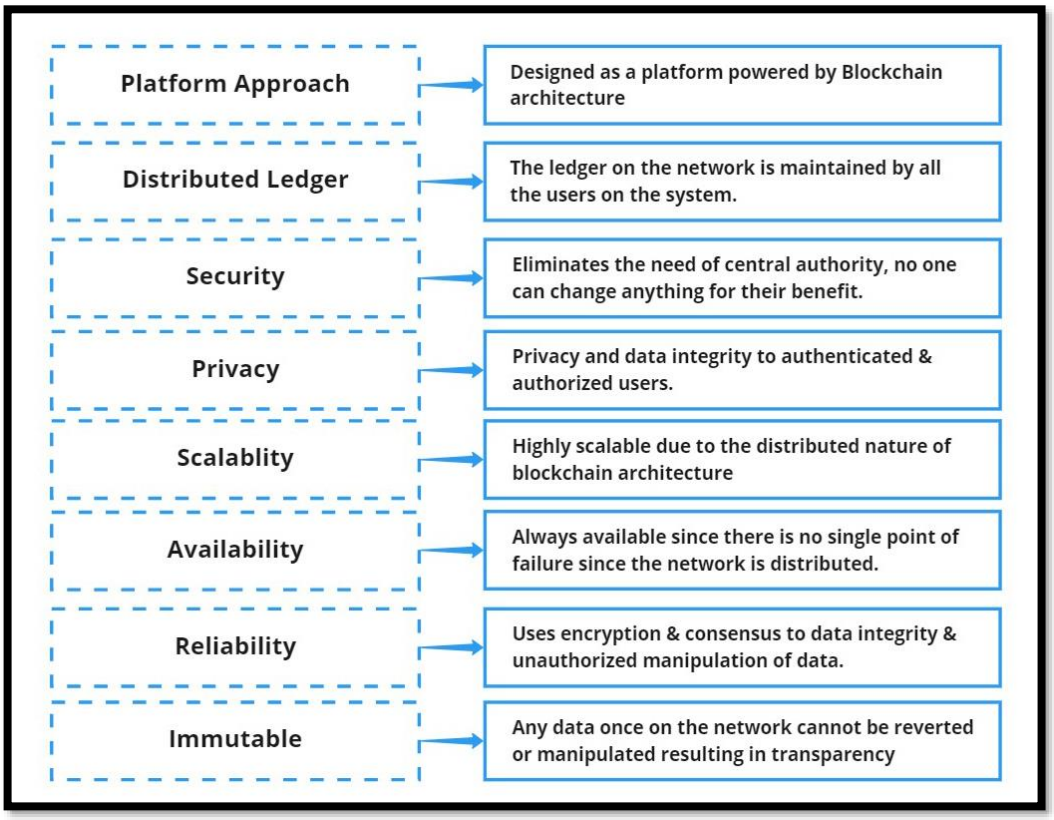
Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., & Imran, M. (2019). An Overview on Smart Contracts: Challenges, Advances and Platforms. Future Generation Computer Systems. https://doi.org/10.1016/j.future.2019.12.019

Appendices

Appendix 1: Technology Backbone for OHIN

Key Solution Design Principle

Figure 19 Key Solution Design Principles of OHIN using Blockchain technology



Platform Approach

A platform approach leverages the value of digital technologies based on IT-enabled interactions. The platform's core consists of a modular structure that allows the firm to

generate a wide configuration of product-service solutions characterized by easily interchanged modules.[142]

Distributed Ledger

A distributed ledger is also known as a shared database synchronized by people across numerous locations, institutions, or geographies. It allows for public "witnesses" to be present during transactions. Each network node's participant has access to the recordings held in common across the network and can own an exact duplicate of them. Any changes, additions to the ledger are instantly reflected and copied to all participants.[143]

Security

It's based on principles of cryptography, decentralization, and consensus, which ensure trust in transactions. In most Blockchains or distributed ledger technologies (DLT), the data is structured into blocks, and each block contains a transaction or bundle of transactions.[144] It is also immutable, so there is no risk of data tampering by anyone for their benefit.

Privacy

Blockchain transactions give users control over their data, allowing them to own it using private and public keys. Third-party intermediaries cannot obtain or misuse data. Personal

[142] A platform approach in solution business: How platform openness can be used to control solution networks - ScienceDirect. (n.d.). Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0019850118303432

[143] Distributed Ledgers Definition. (n.d.). Retrieved from https://www.investopedia.com/terms/d/distributed-ledgers.asp

[144] What is Blockchain Security | IBM. (n.d.). Retrieved from https://www.ibm.com/topics/blockchain-security

data owners can control when and how a third party can access it if stored on the Blockchain. Blockchain ledgers include an audit trail by default, ensuring that transactions are accurate.[145]

Scalability

Private Blockchain is easily scalable due to the usage of efficient consensus algorithms like Proof-of-Authority (PoA)

Availability

The underlying Blockchain network, which is made up of a large number of geo-distributed nodes that maintain a replicated ledger around the clock, ensures availability.[146]

Reliability

Even if some users are hacked, as a whole, the database remains safe because copies of the data are in everyone's hands. Beyond its original objective of assisting digital bitcoin transactions, Blockchain technology has grown in popularity due to its tamper-proof, decentralized nature.[147]

Immutable

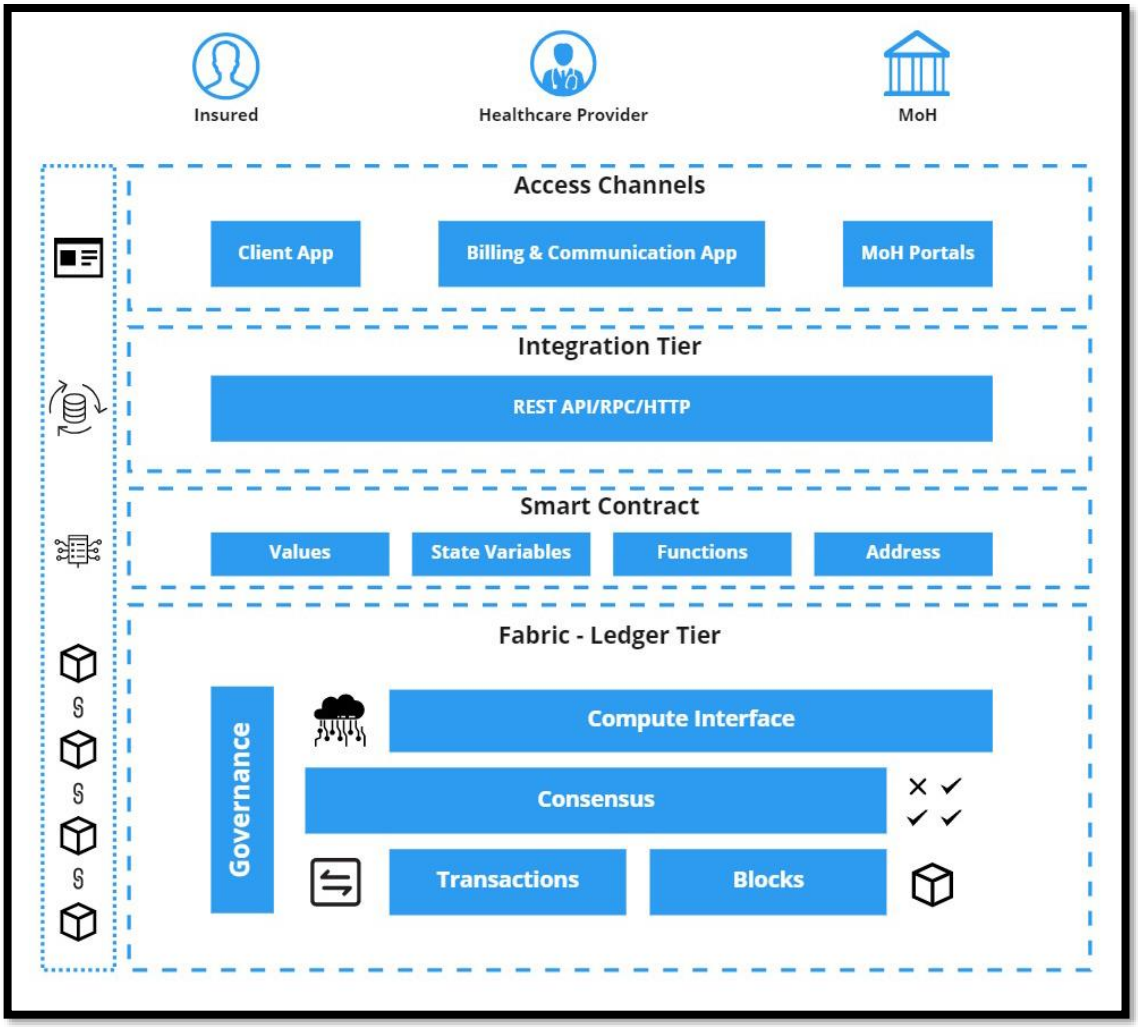
All the data once uploaded to the Blockchain cannot be modified or deleted by anyone.

---

[145] Kshetri, N. K. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 41(10), 1027–1038. https://doi.org/10.1016/j.telpol.2017.09.003
[146] On Availability for Blockchain-Based Systems. (n.d.). Retrieved from https://www.researchgate.net/publication/320651459_On_Availability_for_Blockchain-Based_Systems
[147] Security Risks & Concerns for Blockchain Cryptocurrencies. (n.d.). Retrieved from https://www.businessinsider.com/cryptocurrency-blockchain-security?IR=T

OHIN Solution Architecture

Figure 20 Proposed OHIN Solution Architecture



OHIN Solution architecture consists of 4 main tiers:

<u>Access Channels</u>

This acts as the access point to the entire OHIN, where all the entity of the network communicates or interacts with the network. It transmits the external inputs or data from the entities to the network. The three main access channels in OHIN are:

Client App: It's the application where the Insured makes an online appointment, acknowledges the claims, views drug prescription & lab reports, and views all claim history.

Billing & Communication App: It's the application where the healthcare provider uploads all the claim and supporting documents to the network to initiate the claim process.

MoH Portal: It's the application where the Ministry can audit all the transactions on the network and also resolve disputes in the claim process.

Integration Tier

The Integration Layer is a crucial enabler for a *Service-oriented architecture (SOA)*. It can mediate, including transformation, routing, and protocol conversion to transport service requests from the service requester to the correct service provider. Thus, it supports the capabilities required for enabling SOA such as routing, protocol support and conversion, messaging/interaction style, support for the heterogeneous environment, adapters, service interaction, service enablement, service virtualization, service messaging, message processing, and transformation.[148] REST or RPC can be used for integrations for the access channels to Blockchain.

Smart Contract

Smart Contract is the critical tier of the entire network; the smart contract controls the claim process and disburses the claims based on the pre-agreed terms hard coded into it. It takes

[148] Why the Blockchain is So Secure - open source for you. (n.d.). Retrieved from https://www.opensourceforu.com/2019/05/why-the-blockchain-is-so-secure/

in values from the various external data and is based on which the state variables are set, and suitable functions are executed to process the claim.

Fabric – Ledger Tier

Ledger provides a verifiable history of all successful state changes (valid transactions) and unsuccessful attempts to change state (invalid transactions) occurring during the system's operation.[149] Signed transactions between peers at the most basic level of this infrastructure are available. These agreements between two parties may involve transferring physical or digital assets, completing a task, or other activities. This transaction is signed by at least one participant and distributed to its neighbours. Any entity that connects to the Blockchain is referred to as a node. Full nodes, on the other hand, are nodes that verify all of the Blockchain rules. These nodes organize transactions into blocks and are in charge of determining which transactions are valid and which transactions should be included in the Blockchain and which are not.[150]

For example, a valid transaction in the case of cryptocurrency means Mike obtained one bitcoin from Arthur. However, because bitcoin is a digital asset, Alice may have attempted to transfer the same bitcoin to Carol. As a result, the second Consensus layer requires nodes to agree on which transactions should be kept in the Blockchain to ensure no corrupt branches or divergences.[151]

---

[149] Architecture Explained — hyperledger-fabric docs master documentation. (n.d.). Retrieved from https://hyperledger-fabric.readthedocs.io/en/release-1.3/arch-deep-dive.html

[150] *Classification and main characteristics of blockchain networks. | Download Table*. (n.d.). Retrieved from https://www.researchgate.net/figure/Classification-and-main-characteristics-of-blockchain-networks_tbl1_329136952

[151] Ibid

Blockchain can now offer more functionality thanks to an additional layer called the Compute Interface. In practice, a Blockchain stores a state that includes, for example, all of the users' transactions, allowing for the calculation of each user's balance. However, for more advanced applications, there is a need to store complex states dynamically updated using distributed computing, such as states that shift from one to another once specific criteria are met. SCs, which use Blockchain nodes to execute contract terms, have arisen due to this requirement.[152]

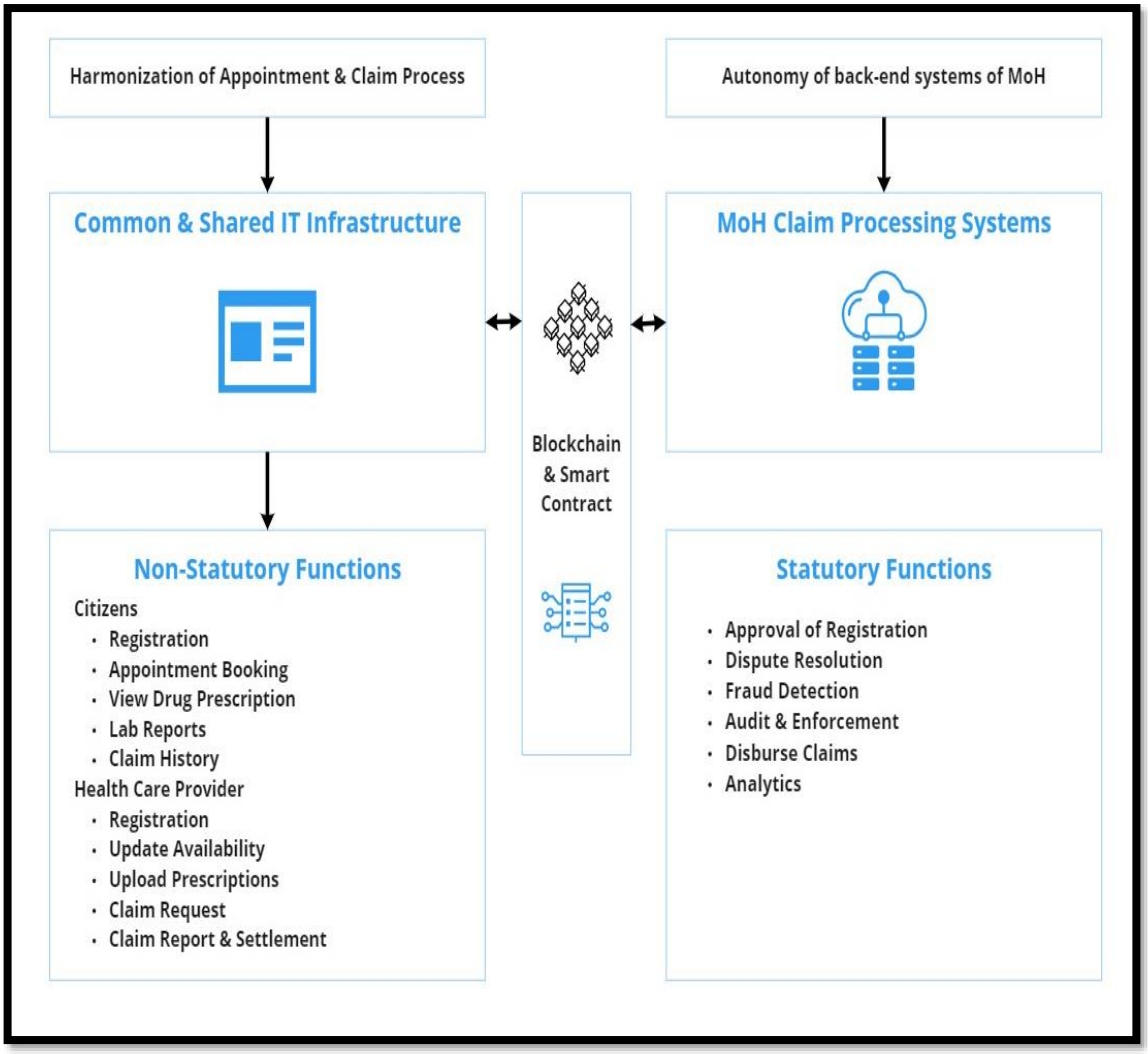
Finally, the Governance layer broadens the scope of the Blockchain architecture to include human interactions in the real world. Even though Blockchain protocols are well defined, they are influenced by contributions from various groups of people who incorporate new methods, improve Blockchain protocols, and patch the system. While these components are necessary for each Blockchain's growth, they are off-chain social processes. As a result, Blockchain governance is concerned with how these various actors collaborate to create, maintain, or alter the inputs that constitute a Blockchain.[153]

[152] *Classification and main characteristics of blockchain networks. | Download Table*. (n.d.). Retrieved from https://www.researchgate.net/figure/Classification-and-main-characteristics-of-blockchain-networks_tbl1_329136952

[153] Ibid

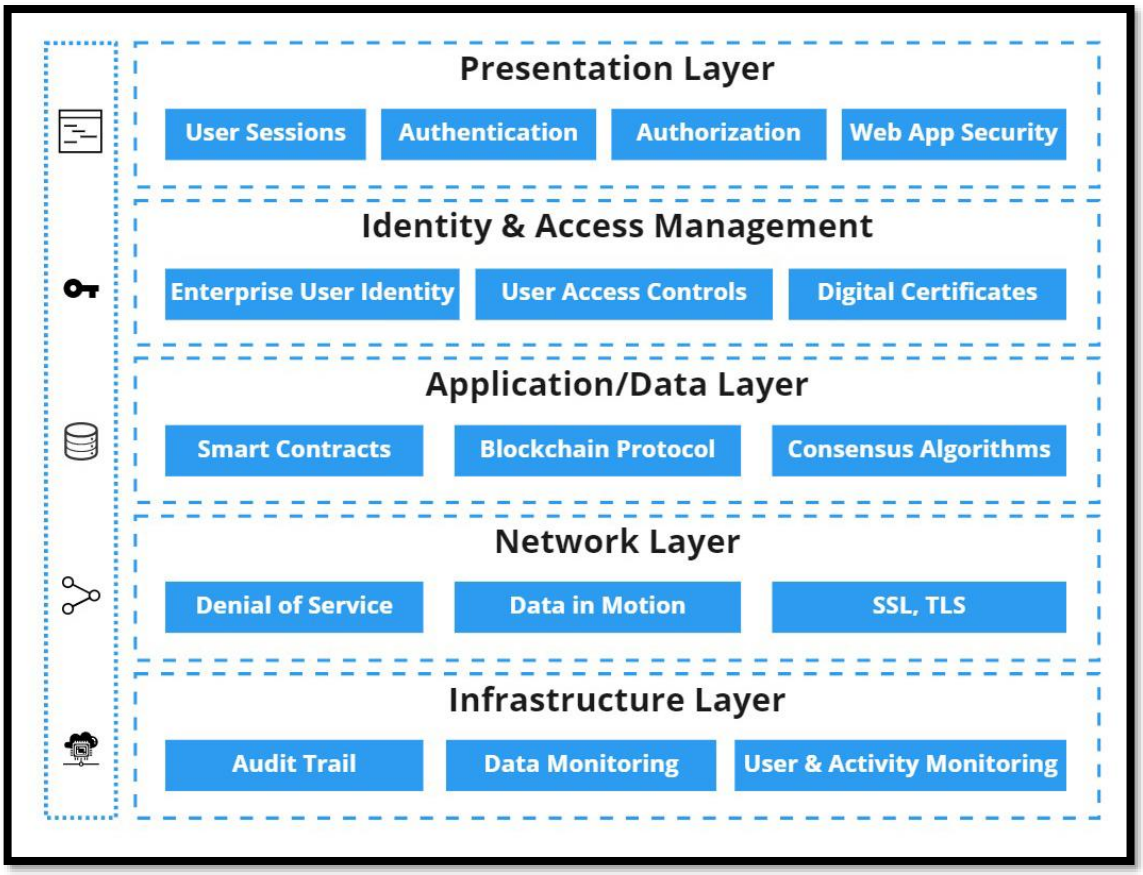
OHIN IT Strategy

Figure 21 Proposed OHIN IT Strategy



OHIN Information Security Framework

Figure 22 Proposed OHIN Information Security Framework.



Presentation layer: It is the front-end where all the entities interact with OHIN

User Sessions: Session security is an essential consideration in designing any system that requires communication between a server and a client.

Authentication: A subscriber's assertion to prove his or her identity is known as authentication.[154]

[154] Why the Blockchain is So Secure - open source for you. (n.d.). Retrieved May 25, 2021, from https://www.opensourceforu.com/2019/05/why-the-blockchain-is-so-secure/ Accessed in April 2021

The authentication factor in OHIN is a Health card number and a password.

Authorization: Authorization is a process to establish the right to perform transactions (actions) and claim access to assets and resources by a subscriber.[155]

Web application security: Web application security should include protection against vulnerabilities identified in OWASP (Open Web Application Security Project) Top 20.[156]

Identity and access management layer

A digital identity is a one-of-a-kind representation of a person or thing that is participating in a digital transaction.

Enterprise User Identity: Verify the user communicating with the system

User Access Control: Grant access to the enterprise assets that users and devices have rights to in each network.

Digital Certificate: An electronic "password" that allows a person, organization to exchange data securely over the Internet using the public critical infrastructure (PKI).[157]

Application/data layer

[155] Why the Blockchain is So Secure - open source for you. (n.d.). Retrieved May 25, 2021, from https://www.opensourceforu.com/2019/05/why-the-blockchain-is-so-secure/ Accessed in April 2021
[156] Ibid

[157] What is Digital Certificate? | Definition of Digital SSL Certificates. (n.d.). Retrieved from https://www.comodo.com/resources/small-business/digital-certificates.php

Calls to the unknown, meaningless send, anomaly disorders, type casts, re-entrants, hiding things, immutable bugs, a value lost in the transfer, and stack size limits are all things that smart contracts and the Blockchain processing platform are vetted for.

The seed (genesis) block is safeguarded, and timestamps are adequately protected. Blockchain guidelines are vetted to discourage the Blockchain from not converging as expected or into an unpredictable state.

Consensus algorithms facilitate transparency by imposing a transaction order that must be accurate for a new block added to the Blockchain to be valid. This ensures that all nodes accept the recent transactions inserted into the block in the network.[158]

Network layer

Denial of Service: A denial-of-service attack, also known as the (DoS attack) is a cyber-attack. The perpetrator intentionally attempts to make a machine or any network resource unavailable to its intended users. It is done by disrupting the services of a host connected to the Internet, either temporarily or indefinitely.

Data in motion: It's data that's openly moving from one place to another, such as over the internet. Firewalls and network access control are examples of network security solutions that can help protect data transmission networks from malware attacks and intrusions.[159]

[158] Why the Blockchain is So Secure - open source for you. (n.d.). Retrieved May 25, 2021, from https://www.opensourceforu.com/2019/05/why-the-blockchain-is-so-secure/ Accessed in April 2021

[159] Data Protection: Data In transit vs. Data At Rest | Digital Guardian. (n.d.). Retrieved from https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest

SSL, TLS: The SSL/TLS protocol encrypts internet traffic of all types, making secure internet communication.[160]

Infrastructure layer

Audit trail: The audit trail refers to all the transactions that the Blockchain will keep track of. The consensus system onboard will oversee transaction ordering and approval. This helps to ensure that the transactions are accurate and visible to other network participants/nodes. [161]

Data protection: Data protection is a crucial process of safeguarding critical information or data from either corruption, compromise, or loss. As Blockchain is immutable, data cannot be compromised, and appropriate measures like redundancy can protect it from corruption and loss.[162]

User and activity monitoring: On Blockchain, all transactions which are valid and performed by users can be tracked. The membership service that comes with the Blockchain will handle user onboarding and management. [163]

[160] What is SSL, TLS? And how this encryption protocol works | CSO Online. (n.d.). Retrieved from https://www.csoonline.com/article/3246212/what-is-ssl-tls-and-how-this-encryption-protocol-works.html

[161] Why the Blockchain is So Secure - open source for you. (n.d.). Retrieved May 25, 2021, from https://www.opensourceforu.com/2019/05/why-the-blockchain-is-so-secure/ Accessed in April 2021

[162] Ibid

[163] Ibid

Appendix 2: Bill 138, Schedule 15

Summary of Amendments Before and After – Impact on Physicians[164]

ORIGINAL BILL	AMENDED
Direct Recovery by OHIP Without a formal hearing, the government would have the ability to recover amounts paid to a physician if OHIP determined amounts were owing.	Schedule 15 now requires a decision of the Review Panel under the Health Services Appeal and Review Board (HSARB) making a finding against a physician before billings can be recovered.
Onus on Proof on Physicians Physicians must prove they have not billed improperly instead of the government proving its claim.	The explicit reference to onus has been removed from the Schedule.
No Ability to Stay Penalty Physicians who sought to appeal decisions of HSARB would have to pay all financial penalties pending appeal instead of staying or delaying the fine until the matter was concluded correctly.	This has been removed from the Schedule.
Review by Non-Peers Anyone could be an inspector and attend physicians' offices to collect and inspect records.	The Schedule has clarified the government's intention to ensure peer-review – only physicians can attend physician offices and review records.
Composition of Review Board Billing matters will be heard by a panel of one physician and two non-physicians.	The composition of the Review Panel will consist of 3 members, including one physician (to provide clinical expertise) and at least one lawyer (to provide expertise in procedural fairness).
Extrapolation/Statistical Inference The government would use statistical inference to determine reimbursement amounts over a specific period before the matter is heard.	The government cannot unilaterally approve the use of statistical inference through direct recovery. Instead, the Review Panel can use statistical methods to recover improper billings, but only where it makes a finding against a physician and only where it is satisfied that it is appropriate to do so.

[164] Bill 138, Schedule 15 Summary of Amendments Before and After-Impact on Physicians ORIGINAL BILL AMENDED Direct Recovery by OHIP Without a formal hearing. (n.d.) Retrieved from https://content.oma.org/wp-content/wp-private.php?filename=Bill-138-Amendments-Summary-2019-Final.pdf

Limitation Period The government could seek recovery over any two years. This would only be applied from the proclamation date in the future (i.e., the government cannot apply this new legislation to billings submitted before these amendments come into force).	The Schedule has been amended to state physicians can only reimburse the government for a 2-year period that does not go past five years from the date the government requested a review. The go-forward window remains.
Disclosure of Personal Information Personal information about a physician who is audited could be published.	The Schedule has clarified the government's intention not to publish information related to a reimbursement hearing or the fact that it believes a physician has improperly billed.

Appendix 3: Interview Questions[165]

1. Do you think your proposed concept for an annual statement to patients will improve transparency and even raise patient awareness? How, in your opinion, can this be implemented?

2. Access to Personal Claims History (PCH) as provided by the Ministry of Health is an alternative. Is this, in your opinion, an effective form of disclosure? Link: https://www.health.gov.on.ca/en/public/programs/ohip/phi_access/default.aspx

3. Do you believe that further action is needed to improve accountability in the OHIP billing and claim process? What, in your view, is the optimal course of action?

[165] As emailed to Mr. David Musyj and reply received on May 25, 2021