Waitematā
District Health Board
Best Care for Everyone

DHB Board Office
15 Shea Terrace
Takapuna, Auckland 0622
Private Bag 93-503, Takapuna
North Shore City 0740
Telephone: 09 486 8900
Facsimile: 09 486 8924
www.waitematadhb.govt.nz

9 July 2020

Amy S Van Wey Lovatt
fyi-request-12922-4e5afdf5@requests.fyi.org.nz

Dear Amy

Re: OIA request – DHB policy regarding the reporting of unsafe or criminal behaviour

Thank you for your Official Information Act request which was partially transferred by the Ministry of Health (MoH) to Waitematā District Health Board (DHB) on 23 June seeking information about our policies regarding the reporting of unsafe or criminal behaviour.

Before responding to your specific questions, it may be useful to provide some context about our services.

Waitematā DHB serves a population of more than 630,000 across the North Shore, Waitakere and Rodney areas, the largest and one of the most rapidly growing DHBs in the country. We are the largest employer in the district, employing around 7,500 people across more than 80 locations.

In addition to providing services to our own population, we are also the metropolitan Auckland provider of forensic psychiatry, child disability services, child community dental services and community alcohol and drug services.

In response to your request, we are able to provide the following information:

1. I was quite concerned and perplexed by the response I received from the MoH dated 16 June 2020 in regards to my OIA request for incident reporting by DHBs. According to Right 4, clause 2, of the Health and Disability Commissioner (Code of Health and Disability Services Consumers' Rights) Regulations 1996: Every consumer has the right to have services provided that comply with legal, professional, ethical, and other relevant standards.

New Zealand Medical Association has provided the Code of Ethics which outlines the professional behaviour that every NZ medical practitioner is supposed to adhere to. Clause 34 of the Code of Ethics states: Doctors have a general responsibility for the safety of patients and should therefore take appropriate steps to ensure unsafe or unethical practices on the part of colleagues are curtailed and/or reported to relevant authorities without delay.

Thus, if there is a legislative requirement that medical practitioners adhere to the "ethical standards", then they must adhere to the NZMA Code of Ethics. In order to comply with the Code of Ethics, doctors must be made aware of the relevant authority in which they must, without delay, report "unsafe or unethical practices on the part of colleagues". The Ministry of Health is ultimately responsible for all DHBs and thus is ultimately responsible to ensure

that all doctors working in DHB's are aware of the "relevant authorities" that they must report to, as required by statute.

[Question 2 transferred to DHBs, below.]*

If you need to consult with the State Services Commissioner, or any other agency, for additional information as to the lawful requirements, standards, and best practices that DHBs, as State Services, must adhere to with regards to Integrity and Conduct, then I would be happy to provide the MoH with additional time to find the requested information.

The MoH will respond to this aspect of your request.

***2. Thus, again, I reiterate my request. I respectfully request a list of all of the "relevant authorities" to which physicians must report "unsafe or unethical practices", with the understanding that criminal behaviour would be included under either "unsafe or unethical practices".**

I also request a copy of all DHB policies in regards to reporting unsafe, harmful, criminal behaviour, including the re-routing and interception of private communications, and policies on how they document such incidents and how they are to safeguard against such incidents, as the Operational Framework does indeed require every DHB to have such policies.

Waitemata DHB's Health Practitioner Competence Assurance Expectations policy **(Attachment 1)** covers the reporting of concerns about the practice of health professionals, including medical practitioners – please refer to.

Waitematā DHB also has a Fraud Monitoring and Management policy **(Attachment 2)** covers the procedures in an investigation of theft or fraud and the reporting of appropriate cases to the Police, Serious Fraud Office or Auditor General.

Our Internet & Email Use policy **(Attachment 3)** states that while security and confidentiality of information cannot be guaranteed when using email, any breach, or suspected breach, must be reported and disciplinary action may be taken.

Medical practitioners are required by the Health Practitioners Competence Assurance Act 2003 to report any concerns about unethical or unsafe practices on the part of another medical practitioner to the Medical Council of New Zealand. Concerns regarding conduct which may be criminal are reported to the Police. The Medical Council of New Zealand's current standards for conduct and professionalism and conduct and competence concerns can be found at: https://www.mcnz.org.nz/our-standards/current-standards/conduct-and-professionalism/

https://www.mcnz.org.nz/our-standards/fitness-to-practise/conduct-and-competence-concerns/

Yours sincerely

Dr Jonathan Christiansen
Chief Medical Officer
Waitematā District Health Board

Health Practitioner Competence Assurance Expectations

Contents

1. Overview

Purpose

This document outlines the particular expectations of health practitioners in relation to the Health Practitioners Competence Assurance Act (HPCAA)

The intent of the HPCCA is public safety to protect the health and safety of members of the public by providing mechanisms to ensure the competence of health practitioners.

Scope

All health professionals working for Waitematā DHB

2. Key requirements

Only health practitioners who are registered under the Act may use the titles protected by the Act or claim to be practising a profession that is regulated by the Act.

All health practitioners must demonstrate competence as established by the professional body.

Concerns about competence must be addressed through coaching and if unresolved reported to the professional body.

3. Scope of Practice

Position descriptions are written to be consistent with the scopes of practice published for the relevant profession.

Health Practitioners must ensure that they act within the defined 'scope of practice' i.e. limitations and self-monitoring and not be permitted to practise outside their scopes of practice.

Health practitioners may only undertake extended practice (beyond a stated scope of practice), if credentialed to do so in accordance with Waitematā DHB policy. Advanced practice extensions or restrictions in the scope of practice must be documented in the employment contract.

Certain activities are restricted and only be able to be performed by registered health practitioners.
Supervision & delegation within the scope

Health Practitioner Competence Assurance Expectations

Delegation of care practices/tasks may only occur within the bounds of the scope of practice of the health practitioner delegated to undertake the work. Senior professionals must provide supervision where a colleague is less experienced or less qualified to undertake the function/task delegated.

4. Competence assessment

Each professional group will have documented nationally consistent competence assessment processes required to show compliance with expectations.

Issue of annual practising certificate certifies that a practitioner is competent to practise within their scope of practice.

- Waitematā DHB will assist professionals seeking to gather the evidence required for these processes.
- All staff will receive an annual performance review and will work co-operatively to establish a constructive performance development management plan.
- Where professions have defined employment requirements and professional requirements these will be supported
- Base requirements are the responsibility of the health practitioner. Waitematā DHB will assist with those requirements that impact on employment e.g. audit, clinical learning opportunities

5. Change in external scope of practice

Where an individual's scope of practice changes e.g. profession directed restrictions or advanced practice training, the health professional is required to inform their manager/clinical supervisor/advisor so that consideration can be given to how the change in external scope of practice may be accommodated. The professional advisor for the service must be included in these decisions with the manager.

See section below on reporting changes.

6. Record keeping

A job description and contract is changed when the position requires, in accord with the recognized competencies and scope of practice. Where there are changes this must be recorded in their personnel file and changes made to their position description and contract.

6.1 Protected Quality Assurance

Professional groups or clinical teams may apply for protected quality assurance status where relevant to review of practice. *Protected Quality Assurance Activity Policy*

6.2 Fitness to practice

Should concern arise about fitness to practice, the manager and professional advisor for the service must follow the accepted process for re-assessment, coaching and performance management.

After all reasonable attempts have been made to remedy such concerns and concerns about fitness to practice remain, referral to the appropriate professional Board will be made in consultation with the General Manager of the service and the relevant professional leader.

All documentation relating to staff referred to their professional Board must be filed formally in anticipation of request for investigation records and the name entered onto the register (see next section).

7. Reporting

7.1 Changes in scope of practice

- It is the responsibility of each health practitioner to advise their manager of any changes to their scope of practice

Health Practitioner Competence Assurance Expectations

- Staff must inform their manager where they have been reviewed by their professional Board for competence or practice issues (whether for an issue when working privately or for Waitematā DHB) and the result of the outcome on their scope e.g. formal supervision.

- Their Board will inform Waitematā DHB as per the legal expectations

8. Competence concerns

Where concerns are identified

Step	Action
1	The peer or manager must bring their concerns to the notice of the service professional advisor to discuss the concern and what the options are. There must be clear documentation of the concerns either as an incident form or audits of practice.
2	The staff member • shall be formally interviewed and advised of the concern • shall receive formal assessment using the professional competencies in order to confirm or refute the concerns.
3	Where appropriate, the staff member shall receive appropriate coaching and/or counselling to allow opportunity for improvement.
4	If concern remains or is confirmed, the health practitioner will be referred to their professional Board as per the approved process.

8.1 Process for referral

Where appropriate, competence or fitness to practice should be referred to the appropriate professional board

Step	**Action**
1	The decision is discussed with key senior staff: general manager of the service professional advisor/leader (e.g. Chief Medical Advisor/ Director of Nursing & Midwifery as appropriate)
2	A letter is written to the professional Board and appropriate evidence provided for their consideration.
3	Detail of the referral is held in a confidential central register maintained by the Quality & Risk Facilitator The full file of evidence must be gathered, organized and formally filed to be retrieved as evidence if required. The Clinical Director or Nurse Advisor holding this information must hold this securely.

9. Associated documents

Type	Title/Description
Legislation	Health Practitioners Competence Assurance Act 2003
Waitemata DHB Policy	Protected Quality Assurance Activities (PQAA)

Waitematā District Health Board
Best Care for Everyone

Fraud Monitoring and Management

Contents

1. Overview

This document sets out Waitematā District Health Board's (Waitematā DHB) policy on fraud. The document gives Waitematā DHB's definition of fraud, its attitude towards fraud and its procedures for identifying and dealing with fraud.

Having the right framework to prevent fraud means having a code of conduct and policies regarding fraud, including protected disclosures, receiving gifts, and using Waitematā DHB credit cards. It means making it safe and easy for staff to talk about fraud and raise any concerns or suspicions. It also means having fraud controls that are reviewed regularly, carrying out due diligence checks of suppliers, doing pre-employment screening, and providing staff with fraud awareness training.

1.1 Purpose

The purpose of this Waitematā DHB document is to convey Waitematā DHB's attitude towards fraud and to:

- Define fraud
- Emphasise the responsibility of staff and management for reducing opportunities for fraud
- Raise staff awareness of the possibility of fraud and its consequences
- Give guidance to employees on the reporting of fraud
- Document procedures for investigation of potential fraud within the organisation.

Fraud Monitoring and Management

1.2 Scope

This policy applies to any irregularity, or suspected irregularity, involving employees as well as suppliers, contractors, outside agencies doing business with employees of such agencies, and/or any other parties with a business relationship with Waitematā DHB.

This document applies to:

- all employees and former employees of Waitematā DHB, including students and volunteers
- all Waitematā DHB Board and Board Committee members
- any person seconded to Waitematā DHB
- any person engaged or contracted under a contract for services to do work for the Waitematā DHB.

For the sake of brevity the terms 'employee' and 'employees' when used in this document include former employees and persons seconded and contracted to Waitematā DHB. This policy uses the term 'fraud' as an umbrella term for the range of possible offences involving dishonesty or deception and encompasses both suspected and proven fraud. Fraud also includes theft, bribery or corruption.

1.3 Associated Documents

Type	Title/Description
Legislation	Crimes Act 1961
	Official information Act 1982
	Privacy Act 1993
	Health Information Privacy Code 1994
	Protected Disclosures Act 2000
	Employment Relations Act 2000
	Crown Entities Act 2004
Waitematā DHB Policies	Protected Disclosures "Whistleblower" Policy
	Discipline & Dismissal Procedure
	Conflict of Interest
Auditor-General's Statement	AG-206: Auditor-General's statement on the auditor's responsibility to consider fraud in an audit of a financial report

2. Policy

2.1 Definition of fraud

For the purpose of this policy Waitematā DHB has adopted the Auditor General's definition of fraud set down in paragraph 11(a) of ISA (NZ) 240, which states:

"Fraud is an intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage."

This definition encompasses but is not limited to:

- False accounting and/or the making of a false or misleading statement or claim with a view to personal gain or gain for another person.
- Knowingly retaining a payment or benefit to which the employee is not entitled.
- Assisting with or condoning fraud or dishonesty against Waitematā DHB by another employee or an external party.
- Theft or unauthorised personal use of Waitematā DHB assets.
- Placing of a contract, or arranging the placing of a contract, with a particular supplier with a view to direct or indirect personal gain.

For the avoidance of doubt "fraud" includes bribery or corruption.

Bribery is the offering, giving, receiving, or soliciting of something of value for the purpose of influencing the action of an official in the discharge of his or her public or legal duties.

Corruption is the abuse of entrusted power for private gain (such as soliciting or receiving gifts or other gratuities).

Theft means to dishonestly, and without claim or right, take or deal with any property with intent to deprive any owner permanently of the property or interest in it.

2.2 Examples of fraud

For the purposes of this policy, examples of fraud include, but are not limited to:

- Payroll frauds, such as falsifying timesheets, leave form or expense claims.
- Accepting and retaining a salary overpayment or leave balance to which the employee is not entitled and deliberately failing to report the overpayment or excess leave.
- Lying about credentials or qualifications.
- Using official position to secure unwarranted benefits, privileges or profit.
- Disclosing confidential information to outside parties with a view to personal gain or gain for another person.
- Accepting or offering bribes or inducements.
- Forgery or unauthorised alteration of any document belonging to the DHB with a view to personal gain or gain for another person.
- Issuing false or misleading purchase orders.
- Approving for payment false or misleading invoices.
- Falsifying invoices.
- Theft of property, records, plant, equipment ,inventory or any item belonging to the DHB, including clinical supplies and equipment, electric devices, office supplies and equipment.
- Unauthorised personal use of Waitematā DHB vehicles or other assets.
- Granting a contract, or engineering the granting of a contract, to a particular company with a view to direct or indirect personal gain.

2.3 Waitematā DHB attitude towards fraud

Waitematā DHB regards fraud as totally unacceptable.

Employees who are found to have committed fraud will be subject to disciplinary procedures. The matter may also be reported to the police and/or the Serious Fraud Office and/or the Office of the Auditor-General for further investigation and possible prosecution.

Recovery of money or property fraudulently obtained will be pursued wherever possible and practicable.

3. Responsibilities

3.1 The Board, Chief Executive Officer and Executive Leadership Team

The Board is ultimately responsible for risk management. In carrying out this responsibility, the Board relies on Senior Management to design and implement effective controls. The Chief Executive Officer (CEO) and Executive Leadership Team, therefore, have the responsibility for the prevention and detection of fraud. They are responsible for ensuring that appropriate effective internal control systems are in place, and that these systems are subject to regular independent auditing.

The Executive Leadership Team are responsible for creating an environment that encourages employees to report suspected fraud without fear of disclosure or retribution, and one where employees believe that dishonest acts will be detected and investigated with appropriate action taken where fraud has been confirmed.

3.2 General Managers / Service Managers / Responsibility Centre Managers

General Managers (GM), Service Managers and Responsibility Centre (RC) Managers are responsible for ensuring effective controls that safeguard against fraudulent activity in their areas of responsibility are implemented and monitored. It is also their responsibility to be aware of common indicators of fraud, identify weaknesses in internal control systems and follow these up with corrective action.

Managers need to ensure employees are informed of, and conform to, applicable policies and procedures and receive appropriate training to enable their staff to have an awareness of common indicators of fraud and to identify weaknesses in internal control. They are also responsible for promoting ethical behaviour within their teams.

As a result of any suspected or actual fraud, senior management must review the implications with regard to internal controls and systems, and implement or amend policies, procedure or controls to prevent similar future frauds. Managers may call on the support of the Regional Internal Audit Service if they require assistance to evaluate or improve internal control systems.

Report any suspected fraud as per section 5.

3.3 All Staff

All Waitematā DHB employees must be scrupulously fair and honest in their dealings with patients, suppliers, contractors, other health service providers and their fellow employees. They must seek the best possible value for the taxpayers' dollars. They must not seek or accept unauthorized personal benefits.

Staff must take reasonable steps to safeguard Waitematā DHB funds and assets against fraud, waste, loss, unauthorised use and misappropriation. Staff members have a duty to report suspected fraud and / or breakdowns in internal control systems to their managers.

A staff member who suspects fraud against Waitematā DHB is expected to report their suspicions as soon as possible as per section 5. Staff are encouraged not to ignore their concerns. All Staff members are entitled to report suspected fraud in accordance with the Protected Disclosures Act 2000 and Waitematā DHB's Protected Disclosures (Whistleblower) Policy.

3.4 Role of healthAlliance

healthAlliance provides the following key services to the Waitematā DHB:

- Finance & Strategy - maintaining the necessary financial disciplines and structures while supporting the delivery of shared services within budget
- Information Services- supporting the delivery of high quality healthcare through technology
- Procurement & Supply Chain services - managing suppliers, contracts and the procurement of clinical / non-clinical goods and services
- Staff Service Centre - providing payroll and human resource management systems

All these services present an opportunity for fraudulent activities. All healthAlliance staff are responsible for reducing opportunities for fraud, and healthAlliance management are responsible for informing the DHB where fraud impacting on the DHB is suspected.

3.5 Role of Regional Internal Audit

The Regional Internal Audit function supports the Waitematā DHB management by reviewing the adequacy and effectiveness of internal control systems. Internal Audit will liaise with relevant bodies to maintain an awareness of current fraud related issues.

The Internal Audit Service is required, as part of its audit programme, to perform regular reviews of transactions, activities or locations that may be susceptible to fraud.

Fraud Monitoring and Management

The steps below are to be followed by the Regional Internal Audit Manager for evaluation and following identification of fraud

1. Where fraud is detected by or reported to the Regional Manager Internal Audit, Internal Audit will immediately report the matter to the CEO, CFO and relevant GM.
2. Internal Audit is required to notify the Office of the Auditor General and/or the Serious Fraud Office of any material instances of fraud. This will be done in consultation with the CFO and/or the CEO.
3. Depending on the strength of the evidence and level of fraud, Internal Audit may recommend to the CFO/CEO or GM that the Police be informed of the fraudulent activity. Involvement of any external parties will be at the CFO/CEO's or GM's discretion.
4. Be part of, or support, the investigation in providing advice on the investigation process and any analysis/review of documentation and/or evidence.

In cases where alleged fraud concerns significant amounts of money and/or has the potential to reflect adversely on the DHB's reputation Internal Audit will:

- Assess the internal controls in the units involved and
- Perform any extended audit work required.
- Report the fraud to the Audit and Finance Committee

4. Internal Controls

Waitematā DHB is committed to the development and maintenance of effective internal control systems to prevent and detect fraud. Examples of internal controls include, but are not limited to:

- Segregation of duties: at least two different people, acting independently, must be involved in the approval of purchasing, finance, payroll and human resources transactions (time sheets, leave applications, expense claims).
- No staff member may purchase an asset for their own, non-work, related use.
- The delegated authority policy states that no employee may exercise delegated authority if they stand to gain personally from the transaction or if they have, or may be perceived as having, some other conflict of interest (for example a family member or some other related party gains from the transaction).
- Performance of thorough background checks when recruiting employees including checking criminal records, checking references and verifying qualifications.
- Due diligence checks to be conducted of any new or potential Suppliers including if relevant that third parties have their own fraud control processes.
- Documentation of financial transactions so that they can be traced through an adequate paper trail.
- Implementation of systems and procedures for verifying timesheets and leave forms.
- Compliance with the Conflict of Interest policy and appropriate declaration of gifts and sponsorship.
- Periodic fraud risk assessments are conducted and a fraud risk control plan developed.
- Regular Fraud risk awareness training is conducted.

5. Reporting suspected fraud

A staff member who suspects fraud against Waitematā DHB should report their suspicions as soon as possible. Staff members are entitled to report suspected fraud in accordance with the Protected Disclosures Act 2000 and Waitematā DHB's Protected Disclosures (Whistleblower) Policy.

Reporting can be as detailed below or via the confidential Health Integrity Line hotline (0800 424 888) or by email to healthintegrityline@moh.govt.nz. All calls are treated with full confidentiality and callers are protected by the Protected Disclosures Act 2000.

Fraud Monitoring and Management

If the staff member suspects fraud by:	They should report it to:	The means by which the allegation will be investigated and documented (including involvement of the Police and/or Serious Fraud Office and/or the Auditor-General) will be decided by:
A contractor, a supplier or an employee of a supplier	Their General Manager. (The GM must report the allegation promptly to the Chief Financial Officer (CFO))	The CFO and/or the CEO after consultation with the Regional Internal Audit Manager.
Another staff member (other than their General Manager or the Chief Executive or the Chief Financial Officer)	Their General Manager. (The GM must report the allegation promptly to the CFO)	The CFO and/or the CEO after consultation with the Regional Internal Audit Manager. HR advice should also be sought.
A General Manager or other Senior Manager/Executive	The Chief Executive. (The Chief Executive must report the allegation promptly to the CFO, the Regional Internal Audit Manager and the Chair of the Board)	The CEO after consultation with the CFO and the Regional Internal Audit Manager. HR advice should also be sought.
If the staff member suspects fraud by:	**They should report it to:**	**The means by which the allegation will be investigated and documented (including involvement of the Police and/or Serious Fraud Office and/or the Auditor-General) will be decided by:**
The Chief Executive and/or the Chief Financial Officer	The Chair of the Board. (The Chair must report the allegation promptly to the Regional Internal Audit Manager and the External Auditor. If there are prima facie indications that the allegation may have substance the Chair must also report it to the Minister of Health)	The Chair after consultation with the Regional Internal Audit Manager and the External Auditor. HR advice should also be sought.
The Chair of the Board and/or another board member	The Chief Executive (The Chief Executive must report the allegation promptly to the Manager of the Regional Internal Audit Service and the External Auditor. If there are prima facie indications that the allegation may have substance the Chief Executive must also report it to the Minister of Health)	The Minister of Health and/or the Office of the Auditor-General

6. Investigation of suspected fraud

6.1 Protocol for Fraud Investigation

In the event that suspicion of fraud arises the following protocol shall be observed.

1. Identifying potential fraud, either by Internal Audit or other means e.g.' whistleblowing'
2. Investigation of the alleged fraud in consultation with the Human Resources Manager, RC Manager and GM. External consultants may be utilised to investigate the allegations.

3. Internal Audit shall report on any implications of the fraud investigation relating to internal controls and systems.
4. Determination on next steps where fraud is established, which may include referral for prosecution and/or disciplinary action.

An accurate and thorough report of the fraud will be prepared. Any documentation or material that could be considered potential evidence should be identified and secured in an unaltered form and kept in a secure location.

No evidence or document should be given to the Police or any other regulatory authority without either the express approval from the CFO / CEO or under the directions of a Court Order.

6.2 Investigations

All allegations of fraud will be consistently and thoroughly investigated with the findings documented. The means by which the allegation will be investigated and documented (including involvement of the Police and/or Serious Fraud Office and/or the Auditor-General) is detailed in section 5. The level of investigation will be proportionate to the level of the fraud. The Director Human Resources and/or Waitematā DHB Legal Advisor should be consulted regarding any investigation in to suspected fraud.

Great care will be taken in the investigation of suspected improprieties or irregularities so as to avoid mistaken accusations. Every individual suspected of committing fraud (whether they are an employee or someone external to the Waitematā DHB) will be dealt with consistently and fairly.

External agencies may be used for investigation if deemed appropriate. Waitematā DHB may also report suspected fraud to the police and/or the Serious Fraud Office and/or the Office of the Auditor-General for further investigation and possible prosecution.

Under the Disciplinary and Dismissal policy, Fraud is classified as serious misconduct. To ensure any disciplinary action is applied consistently to all employees, any investigation into suspected fraud will be conducted in line with the Disciplinary and Dismissal Policy.

6.3 Investigation Team

The CFO / CEO or relevant GM (depending upon the level/significance of the fraud) will allocate the task of investigating allegations of fraud to a person or team.

In cases where alleged fraud concerns significant amounts of money and/or has the potential to reflect adversely on the DHB's reputation, the CFO / CEO shall determine as to whether an external consulting investigators should be recruited.

In any investigation process the Director Human Resources and/or Waitematā DHB Legal Advisor must be involved in the planning and implementation of the investigation to ensure that appropriate employment obligations and all legal requirements are considered.

Internal Audit will defer leadership of the investigation to the relevant manager or Human Resources Manager when it is deemed appropriate. In such cases Internal Audit will maintain an audit oversight. Internal Audit may be required to assist investigators in obtaining information, and should continue to maintain oversight of the investigation.

Others that may need to be involved in a fraud investigation include:

- The Human Resources Manager
- The relevant General Manager
- Police
- Office of the Auditor General
- Legal support and
- Serious Fraud Office

Fraud Monitoring and Management

6.4 Investigation requirements

In order to ensure a robust and comprehensive investigation of any suspected or identified fraud, the following is required:

- Identification of all witnesses
- Review of all systems and documentation as appropriate
- Collation of full facts about the allegations
- Records need to be secured to avoid alteration
- Equipment/assets may need to be retrieved

As a result of the investigation findings:

- Disciplinary action may be necessary
- Criminal prosecution may be necessary
- Restitution may need to be sought for any loss
- Corrective entries may need to be made
- Changes to procedures may be required

Any investigation findings and recommendations will be included in the fraud investigation report.

6.5 Investigation Team Responsibilities

Internal Audit, the relevant investigating manager and the Human Resources Manager will maintain close liaison during the investigation. Information provided or discovered will be held confidentially and securely.

The Investigation Team will make a recommendation to the CFO / CEO and/or the relevant GM as to whether criminal prosecution, civil action and/or disciplinary action should be instigated. The decision to take disciplinary action is the responsibility of the CFO / CEO, GM or Manager of the employee(s) under investigation.

After completion of the investigation, and where appropriate, the investigation team will provide a written report to:

- The Board through the Audit and Finance Committee
- The Chief Executive
- The relevant Senior Manager
- Internal Audit

Internal Audit may also submit a Report to the CEO or GM as a confidential report in which the Auditor independently and freely reports their opinion. Any recommendations made in the report are provided within the consultancy role of Internal Audit.

6.5.1 Investigation Team – Role of Human Resources

The Human Resources Manager will have the responsibility to ensure correct employment procedure is adhered to and will participate in the investigation to the extent required.

Assessment and advice from the Human Resources Manager should involve positioning the Investigation recommendations within the context of employment law and practice, and to this end, legal advice may need to be sought.

During an investigation process the Human Resources Manager will ensure that there is proper support for all employees involved within the applicable Human Resource policies and guidance.

Fraud Monitoring and Management

6.6 Notification

Notifications of fraud investigations and their outcomes are to be made as follows:

The Audit & Finance Committee	To be advised of the outcome of all fraud investigations
The external auditor	To be advised of the outcome of all material fraud investigations
The insurer	To be advised upon discovering a loss or potential loss regardless of whether or not there is a possibility that Waitematā DHB may make a claim on its insurance policy.

Internet & Email Use

Contents

1. Overview

This document outlines the Waitemata District Health Board ("WDHB") policy regarding the usage of the internet and the usage of electronic mail (email).

1.1 Purpose

Internet and email technology is provided by hA on behalf of WDHB as an innovative tool that is integral to WDHB business.

The communication, research and education functions of the internet are recognised and can contribute to the "healthy difference" we can provide for our communities. Email is an important communication tool.

This Internet and Email Use policy is required to:

- Protect the reputation of WDHB
- Protect the integrity and security of WDHB's internal IT systems and applications (including patient and clinical information)
- Ensure that internet and email services are used primarily for business purposes,
- Ensure that emails are stored within the clinical or corporate record in accordance with the Public Records Act 2005 or Health Information Privacy Code 1994,
- Ensure that internet and email services are utilised in a cost effective manner

Internet & Email Use

Because of the evolving nature of both the internet and email, WDHB may modify this policy at any time in order to mitigate risk to the organisations.

2. Policy Components

2.1 Policy Scope

The policy (and associated rules and documents) encompasses and applies to the following components:

- The use of email, both internal and external to WDHB, and related technologies such as internet newsgroups, web or internet based email, instant messaging or other email services
- The use of the internet for the retrieval of information utilising the web browsing software as provided (i.e. Microsoft Internet Explorer, Mozilla Firefox)
- The use of email and / or internet services accessed via a mobile device, including but not limited to, Blackberry, Palm Pilot, tablet or mobile phone.

This policy applies to:

- All WDHB employees (including permanent and temporary), contract staff, students, volunteers, and other users who utilise email or internet as provided by WDHB;
- All resources and devices supplied by WDHB including laptops, mobile phones, internet accounts and modems when used from external locations, such as from home.

2.2 Exceptions

WDHB recognises that periodically there will be a legitimate business requirement that does not comply with existing WDHB policy.

- Where this occurs, a request must be submitted to hA IS via the normal mechanisms (IS Service Desk), however this will require WDHB General Manager or Senior Management approval and in some cases CIO or CEO approval.
- These requests will be assessed and responded to on an exception basis.

It is accepted that clinical or health related images may be held legitimately by health professionals; however some of these may be identified in audits or by other means as meeting criteria for investigation.

Where this material is discovered (or located in the course of an investigation), the user's line manager will assist to determine the legitimacy of the material.

2.3 Monitoring & Disclosure

- WDHB IS systems are provided as a business tool, and while some non-business use is acceptable, WDHB is entitled to access and monitor all information about use, and any material, or information about material, generated or accessed by WDHB employees on WDHB's systems.
- WDHB can be required to disclose information to law enforcement, regulatory agencies, under Official Information Act 1982 requests, and discovery actions in litigation.
- WDHB's Senior Management, Legal Officer or Human Resource Manager can request any information about an individual employee. Internal requests for security, internet or email usage investigations should be submitted to IS Service Desk for a security investigation (without providing the user's details). The resolving team will ask for user details, which are kept outside the Cherwell database for confidentiality purposes.
- No employee should have any expectation of privacy as to his or her internet or email usage. WDHB and hA IS will review activity and analyse usage patterns, and they may choose to publicise this information to the appropriate parties to assure that resources are being used appropriately at all times. WDHB reserves the right to inspect any and all emails or files stored within its network in order to assure compliance with policy. WDHB reserves the right to monitor internet and email use at any time.

- All employees should be aware that systems are in place that record each email message, all internet activity and each file transfer into and out of our internal networks.

2.4 Prohibited Activities

Internet and email is provided for purposes relating to WDHB business including associated research or business related educational activities. Non-business use of the internet and email is subject to all of the conditions detailed within this policy and should be kept to a minimum.

Reasonable non-business use of the internet is permitted. Web browsing using company assets before and after work should be limited to internet banking, non-business emails, news sites and directories (e.g. White Pages).

In addition to this Internet and Email Use Policy, the following activities are prohibited at ALL times and apply to ALL users:

- Users may not use the internet or email facilities to knowingly disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of a patient or another user or system.
- Users may not use the internet or email facilities to knowingly download or distribute pirated software or information.
- Users may not use the internet or email facilities to participate in any form of internet socialising such as dating or chatting. This includes (but is not limited to) such sites and apps as WhatsApp, FB Messenger, Instagram, Twitter, Tinder, Bumble.
- Users may not use the internet or email facilities to knowingly propagate any malicious software e.g. Virus, worm, Trojan horse, hacker tools or trap-door program code, or to obtain information or software intended or designed, disable, overload any computer system or network, or to circumvent any system intended to protect the privacy or security of a patient, another user, or system.
- Users may not use the internet or email facilities to download entertainment software or games, or to play or participate in games against opponents over the Internet or via email.
- Users may not use the internet or email facilities to participate in any form of gambling.
- Users may not undertake any activity that will contravene the laws of New Zealand.
- Users may not undertake any activity that infringes copyright, including (but not limited to) copying electronic files without permission or breaching the terms of any licence.
- Users may not use the internet or email facilities for non-WDHB business, without prior written authorisation from the CEO or other delegated authority.
- All Waitemata DHB business (including patient information) must only be conducted using a Waitemata DHB email account (refer to 2.5) . Staff who work across a number of sites (such as at another DHB or a private practice) must ensure all WDHB related communication is from their WDHB email account.
- Users may not use the internet or email facilities to transmit receive, distribute, view or download offensive, obscene, insulting, harassing, sexist, pornographic or otherwise inappropriate or offensive messages or pictures.

These restrictions apply equally to the use of external instant messaging services such as WhatsApp and Facebook Messenger, external social media apps such as Instagram and Twitter, external email services such as Gmail, Hotmail or Yahoo or those provided by the various internet providers such as xtra, when accessed from WDHB's network or using WDHB resources such as laptops.

The display of any kind of offensive image or document on any WDHB system constitutes a violation of organisational policy.

In addition, sexually explicit material may not be viewed, archived, stored, distributed, edited or recorded using WDHB networks or computing resources, including H: drives.

Undertaking a prohibited activity may be regarded as serious misconduct under WDHB's Discipline and Dismissal policies.

2.5 Security & Confidentiality

hA (on behalf of WDHB) has installed security facilities to assure the safety and security of the networks.

Any attempt to disable, defeat or circumvent these security facilities, including passwords and software licenses, may constitute serious misconduct.

2.5.1 Email and instant messaging

- Security and confidentiality of information cannot be guaranteed when using email or instant messaging services.
- Emails sent between hA, Auckland DHB, CMDHB and WDHB (including all hospitals & remote clinics), travel over a secure, internal link rather than the public internet.
- Private, cloud-based and non-WDHB email addresses are considered non-secure.
- Emails sent to external locations will travel over the public internet potentially allowing them to be intercepted and read by individuals other than the intended recipients.
- Instant messages sent through Facebook Messenger or WhatsApp are stored by Facebook and is not in the DHB's control.
- Secure transmission has been enforced with some external agencies. Refer to the current list on Staffnet – Privacy, Resources List of organisations with secure email link to WDHB

For this reason, commercially or clinically sensitive information should only be sent as follows:

- All Waitemata DHB business (including patient information) must only be conducted from a Waitemata DHB email account (not private email or social media accounts).
- Business emails sent outside the Waitemata DHB network (see above), must be sent either
  a) via a secure external link (only those organisations listed in List of organisations with secure email link to WDHB), or
  b) the commercial/clinical information must be password protected. Refer to password protecting instructions on Staffnet - Privacy, Resources Instructions - Password Protecting Documents . The IS Service Desk can provide further assistance and information on password protecting documents
- For emails **with** patients, see 2.6 below.

2.5.2 Internet

No work-related, commercially or clinically sensitive material or information may be posted on or sent to any web page, internet site or 'blog' page, or through Facebook Messenger or Whatsapp...

2.6 Email Communications with Patients

In the event that a patient indicates that they wish to communicate with a WDHB health care professional by email, the staff member involved must validate the patient's email address and ensure that this is documented in the patient notes.

How to obtain patient consent and to validate the patient's email address is described in the process on the Staffnet – Privacy Respect & Protect – Resources webpage – "Emailing with patients – how to get patient consent and validate an email address".

a) The content of the email communication is part of the clinical record and must therefore be included in the electronic or hard copy notes. Emails to be included in the patient record can either be
   i. copy and pasted into a clinical document where available (eg Paediatrics Progress Note), or

ii. forwarded to ClinicalRecords.mailboxWDHB@waitematadhb.govt.nz with the patient's NHI and the Clinical Records Department will file the email.

b) Where a number of emails are exchanged regarding one matter, and it would be more appropriate for a summary of the email to be recorded and kept, then the health care professional involved must write or dictate a summary. Such summaries should contain the dates the emails span, the number of emails exchanged, who the emails were between, the subject matter, the conclusions reached and advice offered, plus any other relevant information.

c) Summaries must be written frequently so that they are as contemporaneous as possible to the time of the communication. At a minimum, summaries must be written on a weekly basis. All summaries must be written in accordance with the Clinical Documentation policy.

2.7 Breach of Policy

A breach or suspected breach of this policy or any of its components must be reported to the Service HR Manager, CIO or Legal Officer, who will liaise with the hA IS Security Team.

Disciplinary action may be taken for any breach of this policy including minor breaches of a persistent or repeated nature (which will in appropriate circumstances be treated as serious misconduct) as per the relevant Discipline & Dismissal Policies.

3. Internet Use

In addition to the prohibited activities as outlined above, the following applies to all Internet usage:

3.1 Offensive Material

Since a wide variety of materials may be deemed offensive by colleagues, patients, clients or suppliers, it is a violation of WDHB policy to store, view, print or redistribute any document, message or graphic file that is not directly related to an employee's role or a specific WDHB business activity. This will be regarded as serious misconduct under WDHB's Discipline and Dismissal policy

Employees must not download or view offensive, obscene, insulting, harassing, sexist, pornographic or otherwise inappropriate messages, files or pictures.

The display of any kind of sexually explicit image or document on any Employer system constitutes a violation of organisational policy. In addition, sexually explicit material may not be viewed, archived, stored, distributed, edited or recorded using WDHB networks or computing resources, including H: drives.

hA (in discussion with Auckland Region DHBs) reserves the right to block access to potentially inappropriate web sites.

3.2 Courtesy

Due to limited bandwidth, internet users should schedule communication (bandwidth) intensive operations such as large file transfers, video downloads, and the like for off-peak times, generally outside normal business hours (provided these are legitimate work-related activities).

If this is unable to be done outside of business hours, then the IS Service Desk should be advised to ensure system performance can be monitored.

3.3 Social Media

Using social media via internet is also included in this policy. See the Waitemata DHB Social Media Policy for more detail.

3.4 Passwords and Access

Users are responsible for ensuring the security of their access and passwords.

- All passwords must be kept confidential.
- Users must not share their login or password. If a user provides their login or password to another individual or an unauthorised user, they will be held responsible for any actions on their user account, and may face disciplinary action.
- Users should log out of the computer when they have finished using it.
- Users should use a screen saver password to protect access when they are absent from their desk.
- Users should shut down their computers at the end of each working day.

3.5 Downloads

Users may not download any software from any source without hA IS approval.

If software is required for a specific business requirement, this must be requested via the IS Software Request Process, and must be licensed and tested appropriately to ensure legal compliance and to mitigate any risks to the existing infrastructure, systems and data (the users employing service (RC) must provide funding for any licence requirements).

Downloaded software must be used only under the terms of its licence.

Failure to register the software may result in the software and associated data being removed.

Users must not download or attempt to download illegal software licenses or keys (cracks).

- Users may not download mp3s, videos or images without WDHB approval.
- Users may not upload any software licensed to WDHB or licenses or data owned or licensed by any of these organisations without explicit authorisation from the manager responsible for the software or data and hA IS.
- Any files or software that has been downloaded may be used only in ways that are consistent with their licenses or copyrights.

4. Email

In addition to the prohibited activities as outlined above, the following applies to all email usage:

4.1 Email Etiquette

Email is provided as a business communication tool and common courtesy and professionalism should prevail.

Professional and polite language should be used for all business communications, with consideration being given to language and tone.

- It is inappropriate to use email to send heated messages likely to “inflame” the receiver, even if you believe you have been provoked.
- Email etiquette states that messages sent in very large font or in all capital letters is considered to be “shouting” and therefore impolite.
- Do not transmit anything in an email message that could not be sent in writing a letter or memorandum. It is important to remember that the contents of emails are available for redistribution (once sent) and therefore consideration should be taken to the content of the email.

4.2 Public Medium

Communications on the network are often public in nature.

- Please note that because communications originate from the organisation, they can be perceived as being representative of WDHB.

4.3 Forwarding Messages

When forwarding an email message, consider asking the person who sent it for their permission. Act in a professional manner and never alter the original wording.

Internet & Email Use

Automated forwarding of emails to unsecured external email systems is prohibited. This process is of high risk particularly when the emails contain patient or staff information.

4.4 Business Use

Email is primarily for business use.

- Use of the system to solicit or conduct outside business ventures, or to divulge confidential information is prohibited.
- Unreasonable use of emails for non-business buying or selling of goods is not permitted. A Staff Notice Board is provided for this sort of activity.

4.5 Group Exchange Messages

Group exchange messages are a key communication tool within the organisation.

- RC Managers have a responsibility to ensure relevant communications are disseminated to staff in their areas, especially where staff have limited access to these messages.

Group exchange messages to all users are strictly controlled.

- Authority to send group exchange messages must be delegated by the CEO in the normal fashion.
- Group exchange messages to be sent to all users must be forwarded to a staff member with delegated authority for approval.

Group Exchange Messages should not contain attachments unless absolutely necessary.

4.6 Unsolicited Bulk Email (spam)

hA on behalf of the Employers has filters in place to minimise the receipt of unsolicited bulk email, junk mail or spam. Although these filters are very effective in preventing spam, they cannot be perfect. Users must accept that spam is a natural part of using email.

Users must refrain from replying to spam, clicking on or following links contained in spam or from attempting to unsubscribe from bulk email as it seldom does little more than compound the problem.

Do not open or forward chain letters or unsolicited junk emails without first consulting the IS Service Desk.

- It is advisable to delete these items immediately as they may contain viruses or be a virus hoax.

WDHB also reserves the right to automatically block email attachments.

- Should these email be legitimate or expected, the recipient should in the first instance contact the sender and arrange alternative delivery. Spam email is not kept and cannot be released.
- User can contact the IS Service Desk for more details.

Users must not participate in the sending, forwarding or replying to chain emails.

4.7 Software virus control

Virus scanning software is provided as standard on every PC or Laptop within WDHB.

- Ensure that this software is active at all times.
- Be aware that viruses can remain undetected as attachments within emails until those attachments are opened.
- Be aware that viruses can be sent from a person known to the user without their knowledge.

4.8 Limitations

To maintain and limit the ever-increasing burden of electronic information storage, the following limitations are applied to email services:

- Sent or received emails which are greater than 10 MB (megabytes) will be automatically blocked;
- Inbox size should not exceed 45 MB;

By default, automatic archiving of old emails is activated, however, this may be modified if an employee requires the need to retain direct access to old emails.

Internet & Email Use

4.9 Public Records Act 2005 Requirements

Any email that is a business dealing on behalf of WDHB is a corporate record (information created, received and maintained by WDHB to fulfil legal obligations or to evidence business transactions) and as such all corporate records must be stored within the corporate repository in accordance with the Corporate Records Management policy.

5. Reference Information

5.1 Related & Associated Documents

Other documents relevant to this policy/process/procedure are listed below:

Type	Title
NZ Legislation	Various
WDHB Policy & Procedure	• Discipline & Dismissal Policy • Information Security Policy • Information Security Principles Policy • Communications Policy • Social Media Policy • Corporate Information Policy • Clinical Documentation Policy
hA	• IT Acceptable Use Policy • Password Policy

5.2 Definitions

Terms and abbreviations used in this document are described below:

Term / Abbreviation	Description
WDHB	Waitemata District Health Board – including all remote sites and services.
hA	healthAlliance – including all sites and services.
Internet	The term "internet" refers to the global network of publicly accessible computers linked using the Internet Protocol standard.
World Wide Web (WWW or Web)	The terms "World Wide Web" and "Web" refer to Internet servers accessed via the Hyper Text Transfer Protocol (HTTP)
Email	An electronic message transmitted via the internet
IS	healthAlliance Information Services (also know as hA IS)
Spam	Unsolicited bulk email
Offensive material	Any material (including but not limited to images, graphics, videos, sound files, texts, documents or emails) that are or could be deemed offensive or inappropriate. Including but not limited to: • Pornographic / sexual explicit material • Sexist material • Insulting material • Racist or religiously intolerant material • Harassing, bullying or threatening material of any kind.
Employee	Refers to any user of WDHB computer systems and applications including employees, contractors, students.