DIRECT CARE AND TREATMENT

Data Privacy, Data Incidents, and Open Meetings

Data Privacy Office| Direct Care and Treatment

Why do we have a Data Privacy Office?

- State and federal laws require that we keep data safe
  - HIPAA and MGDPA are the key laws to the Privacy Office
- We must report data incidents properly and respond to data requests made of DCT.
- Data ranges from data stored in the cloud to printed pieces of paper at Moose Lake
  - All data in any form must be secure and protected
- Improper data usage will create substantial legal and media issues for DCT

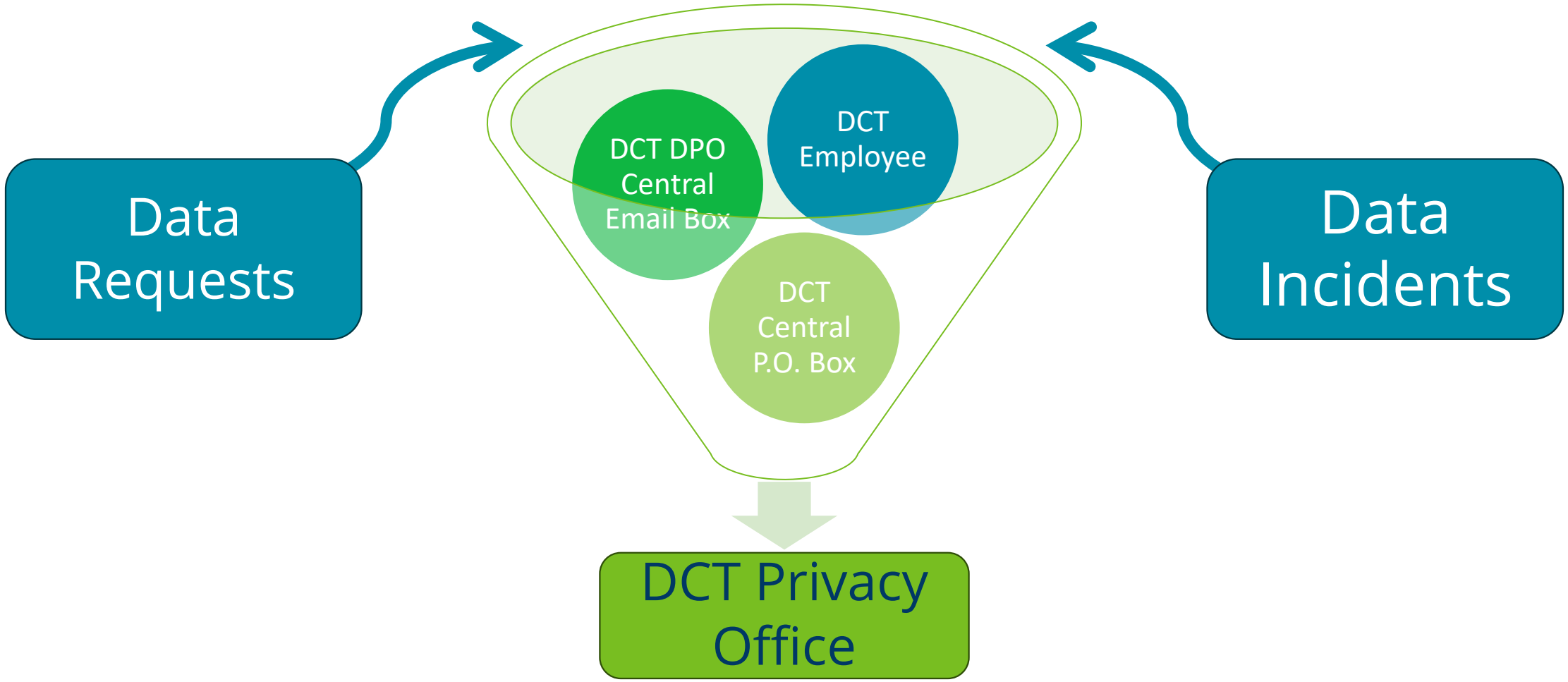
HIPAA - Federal Law

- Health Insurance Portability and Accountability Act (HIPAA)
- Protects medical data of clients
- Ensures medical data can be shared with other providers securely
- Only covers medical data created, shared with, or maintained by health care professionals

MGDPA - State Law

- Minnesota Government Data Practices Act (MGDPA)
- Chapter 13
- What information can be collected
- How the data can be used
- Duties when holding someone's data

How Data Issues Reach DCT Privacy



Defining Data Requests

A “Data Request” refers to a request for government data

- Public government data are available to any requester, for any reason
- A client’s data is available to that client at request

“Government data”

- all data collected, created, received, maintained or disseminated by state or local government, regardless of its physical form, storage media, or conditions of use
- Paper documents, email, CDRoms, videotape, and computer files are all forms of “government data.”

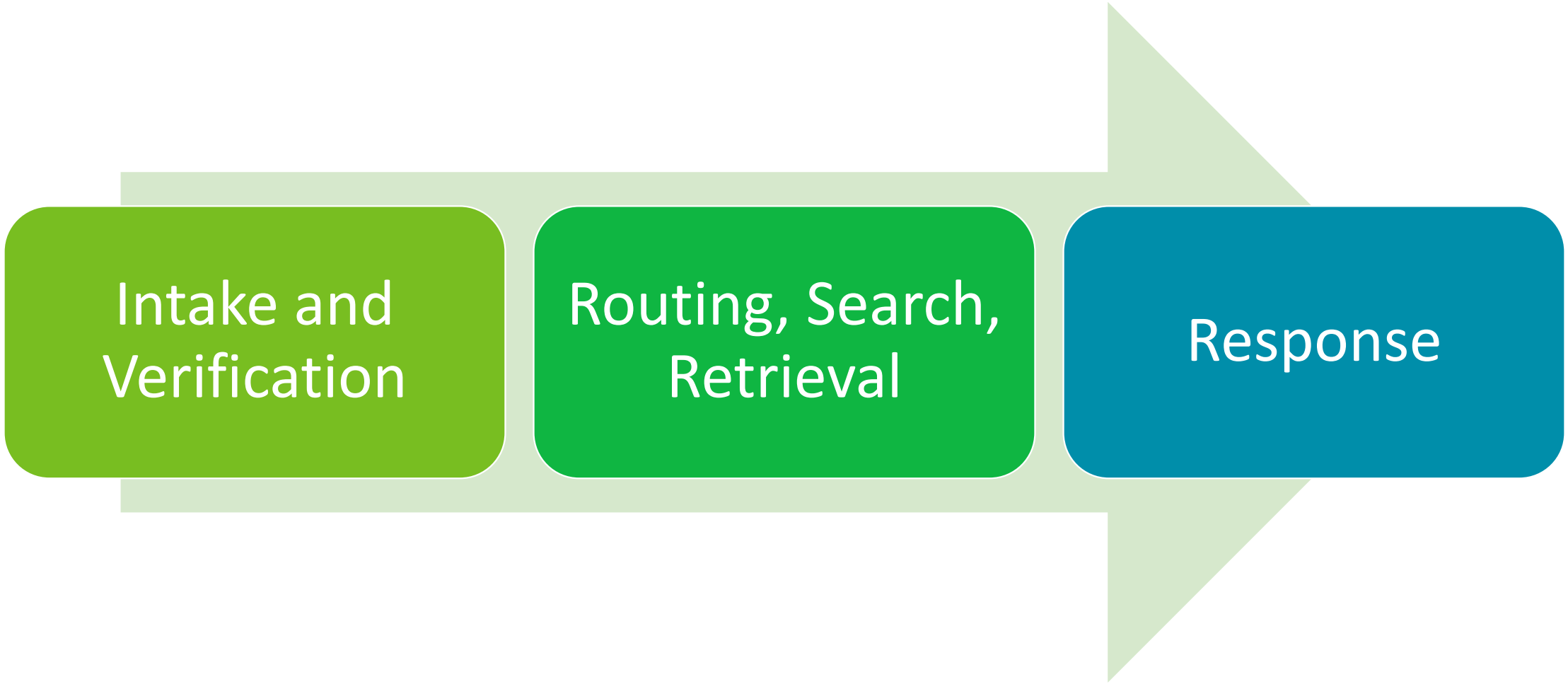
How Data is Classified and Disclosed

Public Data	All government data is considered public unless explicitly classified otherwise by law.
Private Data	Data about individuals that is considered private and can be disclosed to the individual or to limited government entities for limited purposes.
Nonpublic Data	Data not about individuals but also disclosed only to limited government entities for limited purposes.
Confidential Data	Data about individuals that are available only to limited government entities and not available to the individual or the public.
Protected Nonpublic Data	Data not about individuals, but only available to limited government entities and not available to the individual or the public.

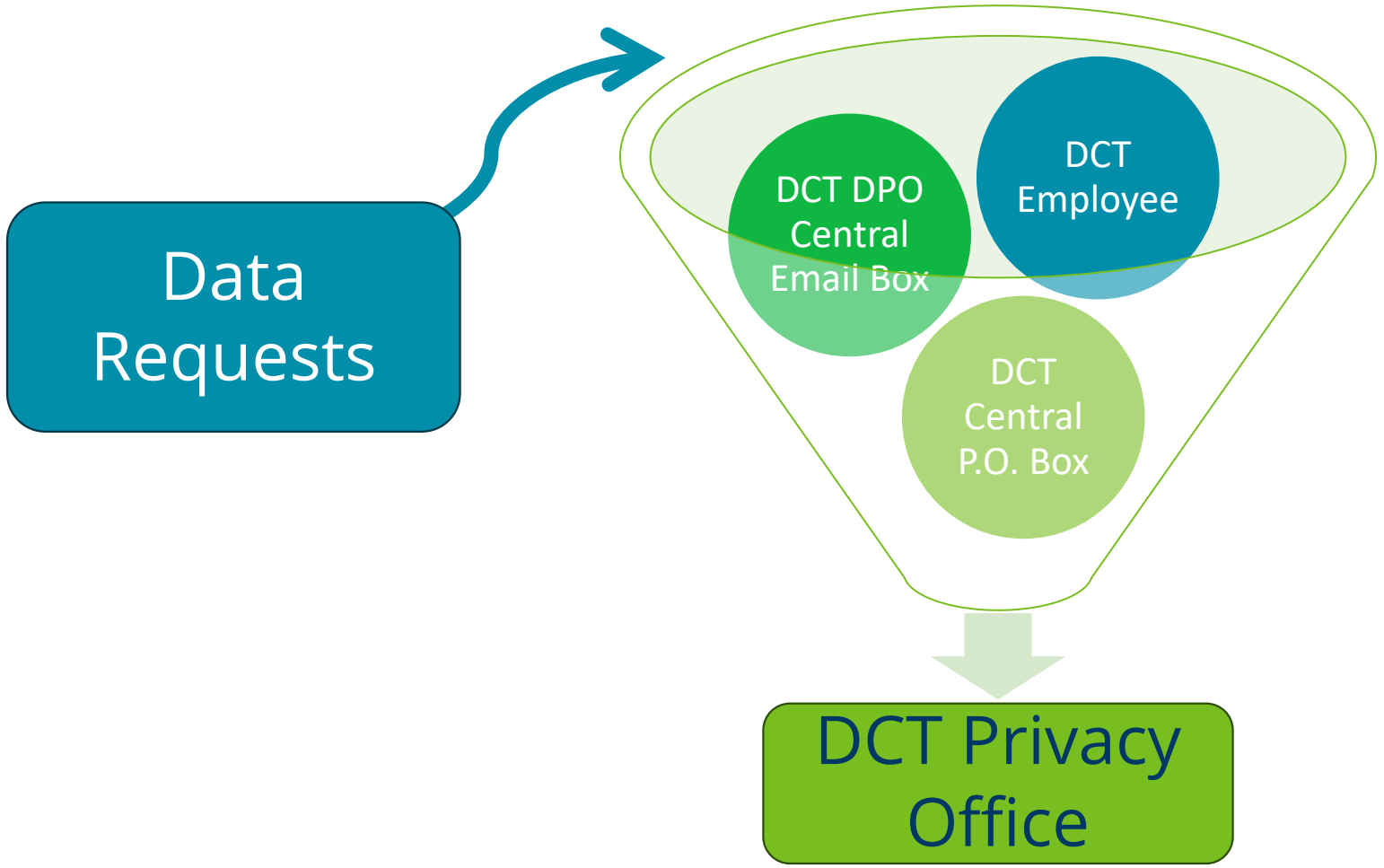
Data Classification Examples

Public	Private	Nonpublic	Confidential	Protected Nonpublic
• All government data unless otherwise classified by law. • Most contracting data • Certain education directory information • Most dates of birth in police reports • Some personnel data • Some applicant data	• Most personnel data • Some security information • Social Security numbers • Some body camera data • Most education data • Certain child abuse data • Certain vulnerable adult data • Contact data provided to the government for notification or subscription purposes	• Some security information • Some body camera data • Certain contracting data	• Certain real property complaint data • Certain active investigation data not otherwise classified • Witness/victim dates of birth in active investigations	• Certain real property complaint data • Certain active investigation data not otherwise classified

DCT Data Requests



How Data Issues Reach DCT Privacy



Verification and Costs

Identify Verification

- The identify of clients must be verified before handing over sensitive data
- This is done via a valid photo ID of the person or their guardian

Charging for Data Requests

- DCT may charge for data requests
- Private requests
  - Only creating and certifying copies costs
- Public requests
  - Search, retrieval, making, certifying, sorting, and transmitting the data cost

Category of DCT employee	Average hourly rate (April 5, 2024)
Administrative staff	$26.79
Information Technology staff	$50.00
Professional staff	$44.75
Managerial staff	$64.44

Routing, Search, and Retrieval

- After verification, DCT Privacy works with the business areas to determine if the requested data exists and where the requested data is located
- DCT Privacy requests the data from the business areas and collects it to return to the individual
    - Each person thought to have data must conduct their own search
    - All data is collected in a shared folder
    - The folder is then reviewed and prepared for the requestor
    - Redactions and citations are added for any data that cannot be shared
        - Includes welfare data, PHI, private personnel data, and many more

If	Then
Business area does not have responsive data.	The Data Liaison will notify the DCT DPO which will respond in writing to alert the requestor.
Business area has responsive data.	The Data Liaison will estimate the costs related to the request and notify the DCT DPO. The DCT DPO will respond to the requestor and request costs, as defined in the estimating costs and payment section of the manual.

Privacy Incidents

A privacy incident occurs when there is an unauthorized **access**, **use**, or **disclosure** of not public data that **identifies an individual**

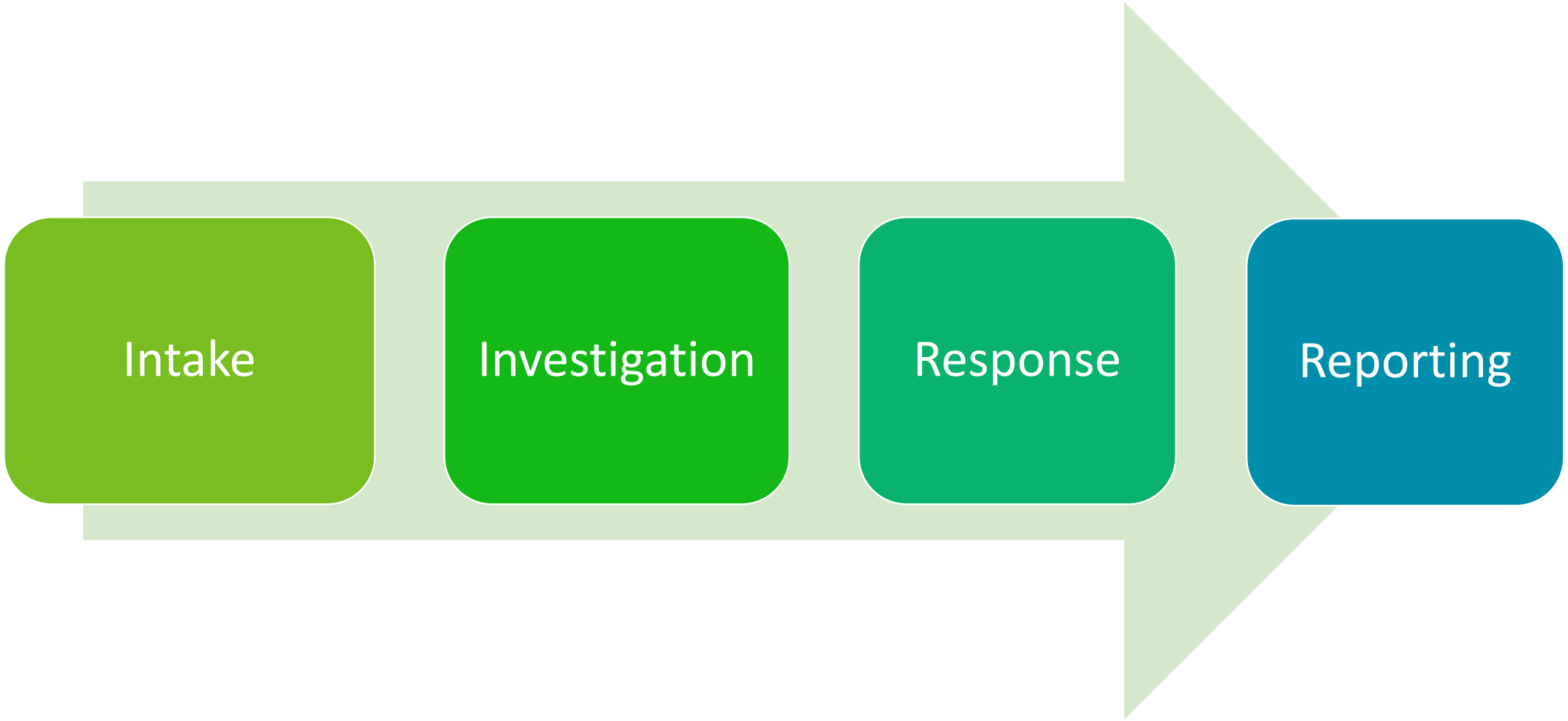
A privacy incident can be **accidental** or **intentional**

Accidental: a misdirected email containing not public data

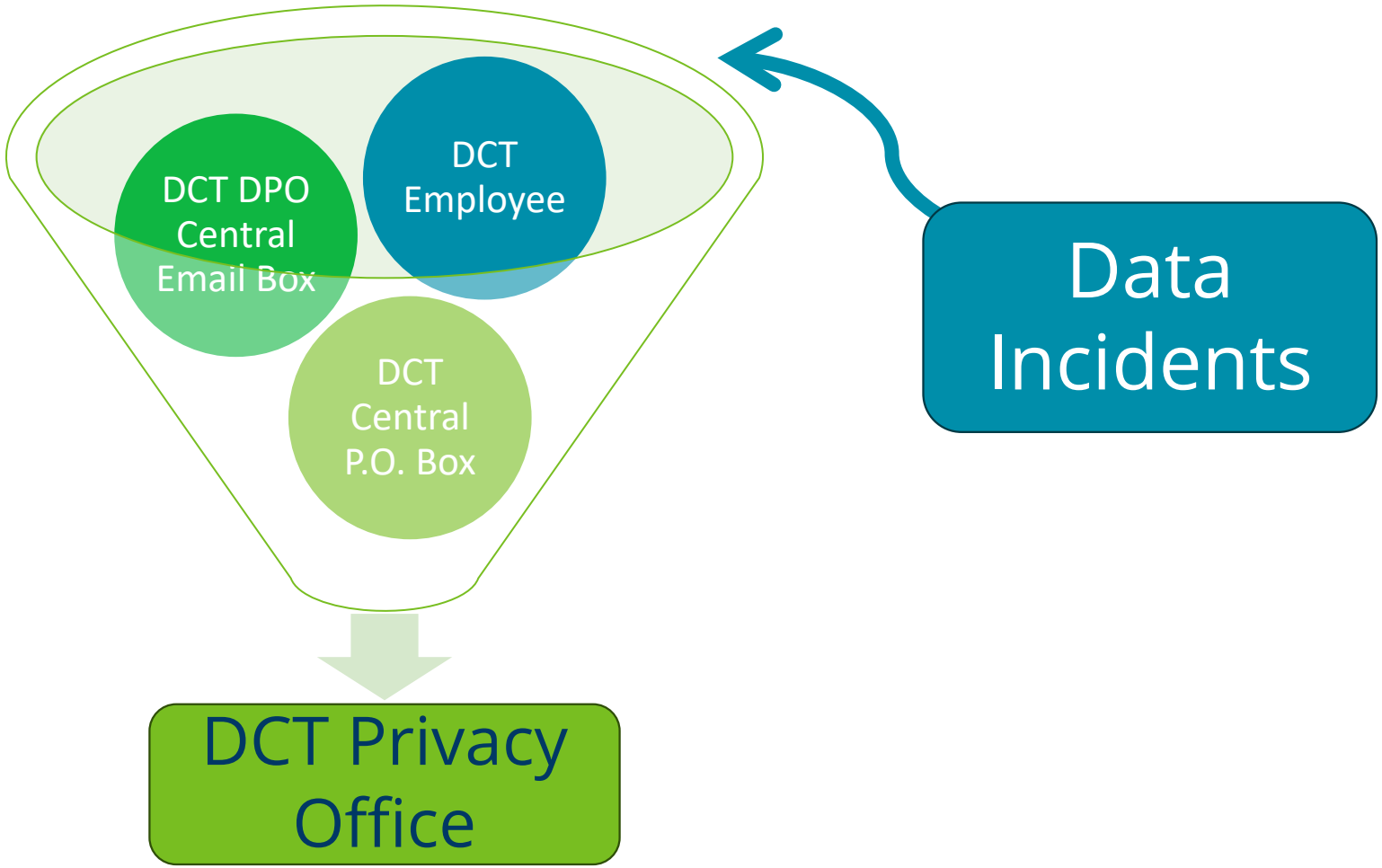
Intentional: an employee accessing records containing not public data without a work purpose

A **data incident** only becomes a **data breach** after a determination by the DCT Privacy Office

DCT Data Incidents



How Data Issues Reach DCT Privacy



DCT Privacy Incident Investigation

DCT Privacy Office creates a file number and works with the incident reporter identified on the Data Privacy Incident Report Form to verify:

- Whose data was inappropriately disclosed?
- To whom was the data inappropriately disclosed?
- What happened to cause the information to reach unauthorized eyes?
- When was the inappropriate disclosure made?
- Where was the disclosure made?
- Why did our safeguards fail to stop the data from being released?
- How do we remedy this incident and how do we prevent it from reoccurring?

Health Insurance Portability and Accountability Act

An analysis of the risk factors shows the probability that the PHI has been compromised:

(i) The **nature** and **extent** of the protected health information involved, including the types of identifiers and the likelihood of re-identification

(ii) The **unauthorized person** who used the protected health information or to whom the disclosure was made

(iii) Whether the protected health information was **actually acquired or viewed**

(iv) The extent to which the **risk** to the protected health information has been **mitigated**

Minnesota Government Data Practice Act Analysis

Analysis of the data on individuals:

(i) An unauthorized person

(ii) obtained, accessed, or viewed

(iii) government data

(iv) without informed **consent** of the individual data subject or statutory authority

(v) with **intent** to use the data for a non-governmental purpose, and such action

(vi) compromised the **security** and **classification** of the data.

DCT Privacy Incident Response

- DCT Privacy works with the business area to investigate and respond to the data incident
- DCT Privacy drafts a letter and assists the business area in sending out the letter
- There is a 60-day time limit to respond to requests
- Records on every data incident are recorded within DCT Privacy
- The breach is reported as necessary

Breach Reporting

- Breaches of MGDPA are reported on a weekly basis to the Office of the Legislative Auditor (OLA).
  - State law requirement
- Breaches of HIPAA are reported to the Federal Office of Civil Rights (OCR)
  - Federal law requirement
- Breaches of HIPAA affecting 500 or more individuals in a geographic area are also reported to the media.
  - Federal law requirement
- How many of each request do you think DCT gets every year?

Data Incidents and Data Requests Quiz

- How many Data Incidents does DCT have every year?
- How many Data Incidents are reported to OLA every year?
- How many Data Request does DCT have every year?

Data Incident and Data Request Yearly Numbers

- 78 Total data incidents in 2024
- 23 Data incidents reported to the OLA
- 10 HIPAA breaches reported to the OCR
- 1 Data breach reported to the media in 2024 under the HIPAA
- 3,600 data request have been made to DCT in 2024
  - Most come from MSOP

Incident Record Keeping

The DCT Privacy tracks the incident in the DCT Data Incident Tracker and keeps files with records of all incidents, including the following:

- Data Incident Report Form
- Breach Analysis Form
- Email Correspondence
- Notices to Data Subjects
- Notices provided to the OCR and OLA
- Minn. Stat. 13.055 Report

General Data Practices

Personal device use is not allowed

- DCT must retain and access all state data
- This includes your personal device
- We will have to look through your devices with state data if there is a litigation issue

Data requests can involve your personal devices

- If data is being stored on your personal device, it may be requested in a data request

Data incidents can involve your personal devices

- If there is a breach through your personal device, DCT may need to look through your personal device to identify what data was leaked
- Data incidents may need to reported to the federal government and media

Questions and Further Information

- Any Questions?
  - Questions about Data Privacy, Data Incidents, and Data Requests

The Open Meeting Law: A High-Level Overview

General Counsel's Office| Direct Care and Treatment

Open Meeting Law

A meeting must be open to the public when "**required or permitted by law to transact public business in a meeting**"

Defining a “Meeting”

- A “meeting” is held when the group is capable of exercising decision-making powers.
  - A quorum is a simple majority of the board
- A meeting is any meeting of members to discuss, decide, or receive information as a group on issues relating to the official business of that governing body.
- Keep public perception in mind.

Gatherings NOT Subject to the Law

- Gatherings of less than a quorum of members
- Chance or social gatherings
- Training or team building activities as long as business is not discussed
- Be careful not to enter a situation where decisions are being considered or information is being gathered
- A chance meeting can become a meeting the moment business is discussed

Why are Open Meetings Required?

1. To prohibit actions from being taken in secret where it is impossible for the interested public to be fully informed.
2. To assure the public's right to be informed.
3. To afford the public an opportunity to present its views to the public body.

Who Must Comply?

- Multi-member groups where decision-making authority lies with the group
- Multi-member groups created by statute where the chair or the administrative support comes from a state agency
- Groups created by the governor
- Groups created by the commissioner of a state department or section 15.014
- Bodies filled under section 15.0597 (Open Appointments Act), or other state law
- Multi-member groups established by a state agency on proposed rulemaking
- Groups with governmental powers (i.e., the power to regulate, license, make public policy, or determine the use of public resources or otherwise transact public business)

Who is NOT Required to Comply?

- Ad-hoc advisory groups convened by division, bureaus or other units of a state agency
- Those not having ultimate decision-making authority (i.e., the commissioner or governor makes final decision)
- Those not required to transact public business in a meeting

Exceptions to the Open Meeting Law

The Open Meeting Law does not apply:

1. To meetings of the commissioner of corrections
2. To a state agency, board, or commission when it is exercising quasi-judicial functions involving disciplinary proceedings
3. As otherwise expressly provided by statute

Required for Open Meetings

Votes

- Record the votes of the members by name of the state agency, board, commission, or department; or of the governing body, committee, subcommittee, board, department, or commission on an action taken in a meeting required by this section to be open to the public must be recorded in a journal or minutes.
- The vote of each member must be recorded on each appropriation of money, except for payments of judgments, claims, and amounts fixed by statute.

Printed copy of the board packet for any member of the public that attends

Meeting Notices

Meeting Type	Notice Requirements
Regular Meeting	Keep a schedule on file at primary offices with the time and place (or web post interactive technology information 10 days in advance) of regular meetings. See MN Stat 13D.04, Subd 6.
Special Meeting	Post written notice of the date, time, place (or interactive technology information) and purpose of the meeting on the principal bulletin board or on the door of the usual meeting room.
Emergency Meeting	Telephone notice provided to news media as soon as members have been notified.
Recessed Meeting (or Continued Meeting)	Record the time and place (or interactive technology information) of the meeting in the minutes of the previous meeting, if it was established in the previous meeting.
Closed Meeting	Requirements for closed meetings are the same for open meetings of the same type.
Virtual Meeting	Meeting notice must include the regular meeting location, that members may participate by interactive technology, and information on monitoring the meeting electronically from a remote location. Must post 10 days in advance on the DCT website.

Closed Meetings

- Meetings can be closed only if required or permitted in the law
- All closed meetings must be recorded (attorney-client exception)
- No general “personnel exception” to close a meeting
- Statement on the record before closing a meeting
  - Legal authority to close the meeting
  - Describe what will be discussed

When Meetings MUST be Closed

Meetings MUST be closed when the following is discussed:

- Data classified as “not public”
- Data that would identify alleged victims or reporters of criminal sexual conduct, domestic abuse, or maltreatment of minors or vulnerable adults
- Active investigative data or internal affairs data
- Educational, health, medical, welfare or mental health data
- Allegations or charges against an individual subject to its authority

When Meetings MAY be Closed

- Meetings closed as expressly authorized by statute
- Meetings closed as permitted by the attorney-client privilege
- Meetings that discuss:
  - Labor negotiations
  - Employee performance evaluations, but the meeting must be open at employee's request
  - Certain property transactions (asking price for property, review of confidential appraisals, develop offers or counteroffers)
  - Certain security matters

How to Close a Meeting

A public body closes a meeting by doing the following:

1. Making a statement on the record
2. Giving the statutory authority that requires or permits closing the meeting
3. Specifically describing what will be discussed at the meeting

Open Meetings Quiz

The board is deadlocked on a time sensitive issue. You decide to email other members to discuss the next steps to resolve this.

How many members may you email at one time before it becomes an open meeting requirement?

- Zero: Emailing a board member at all is a meeting
- 1 member
- 2 members
- 3 members
- 4 members
- 5 members
- 6 members
- 7 members: Only emailing the entire board constitutes a meeting
- Emails are not considered a meeting

Discussing the Answers

- Emails can constitute a meeting
  - A meeting is when a quorum has decision making power
  - This can occur over email

Questions and Further Information

- Any Questions?
  - Questions about meetings

DIRECT CARE AND TREATMENT

Thank You!