BRIGHTSQUID

Practical Privacy:
Keep Indigenous Patient Data Safe in the Real World

Oct. 9, 2024

Jeff MacKay

Tools & Understanding for Clinic Optimization

1. Review findings from privacy survey
2. Privacy risk and resilience
3. Privacy Challenges for Indigenous Healthcare
4. Compliant communication for Indigenous Healthcare
5. Changes in the privacy landscape

Brightsquid?

Founded in Alberta in 2009 by a Radiologist to get patient data where it needs to be quickly and safely.

(Bringing light where there was darkness)

65,000+ Healthcare organizations across North America use Brightsquid Secure-Mail share patient data compliantly.

Privacy compliance consulting for hundreds of clinics, vendors, and authorities.

brightsquid.com

Healthcare gets better when we all work together.

BRIGHTSQUID

Privacy Compliance + Security

Data Security:

Maintain confidentiality, integrity, and availability to protect data from unauthorized access, breaches, and loss

- Encryption
- Access controls
- Part of compliance

"External email is OK if it's encrypted."

Privacy Compliance:

Ensure data is managed according to legal obligations, individual rights, and ethical standards.

- Policies, procedures
- Consent
- Data security

"External email is *never* OK because webmail services sell data for marketing."

Privacy Scan of 25+ First Nations Health Centers

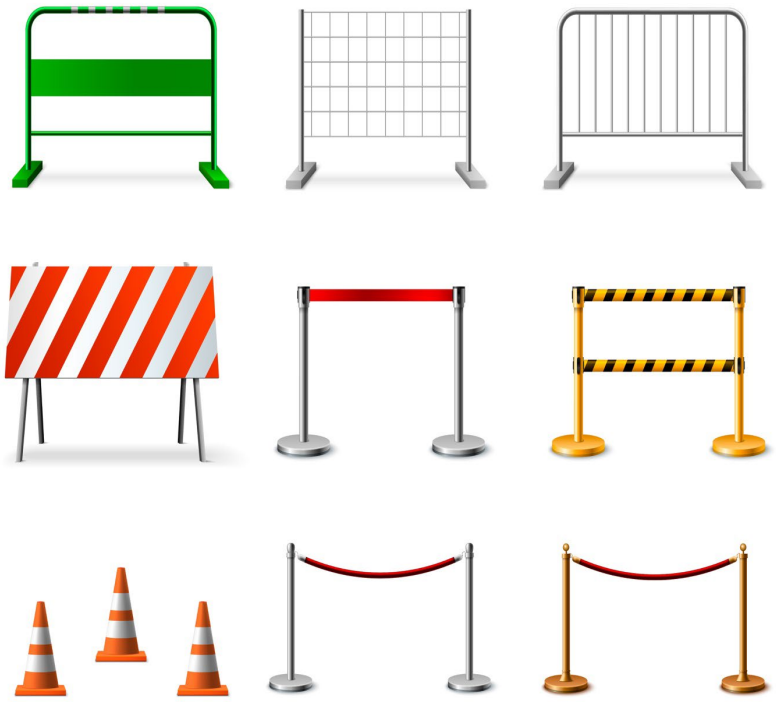
1. Understand general privacy practice and awareness
2. Support full gap analysis and remediation plan
3. Support increase in patient trust and access

BRIGHTSQUID

Findings

Challenges in First Nations Healthcare

- Capacity
  - Overwhelm
  - Resource allocation
- Organizational continuity
  - Who is in charge?
  - What polices? Where?
  - Regulatory up-keep
- Trust & Cultural Safety
- Roles, responsibilities, functions
- Complex mental health
- Transportation (Access)



BRIGHTSQUID

The Good

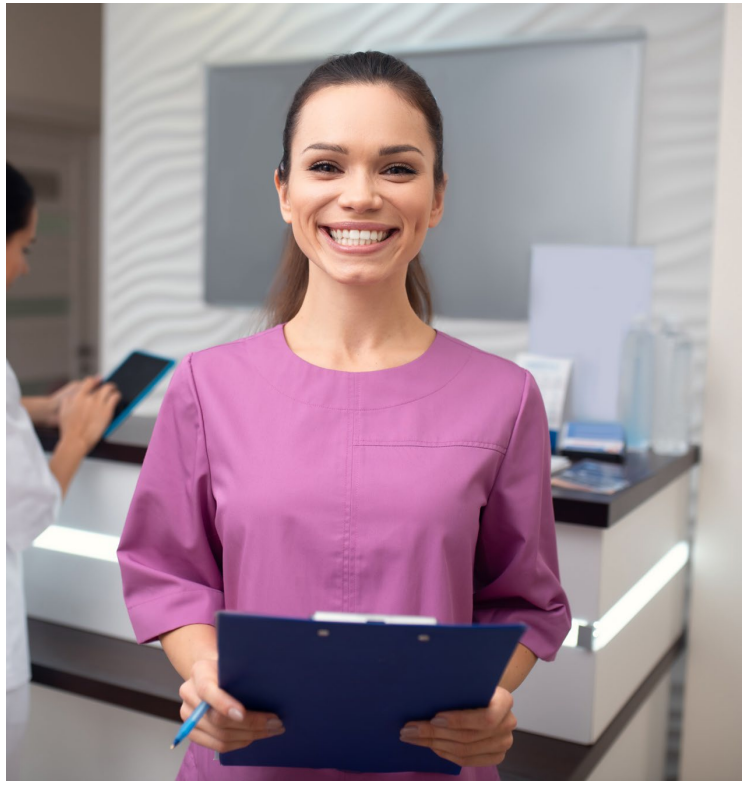
- Staff are aware that privacy compliance is a concern
- Confidentiality oaths are common
- Physical security measures are well established
- Firewalls and VPNs are configured in many locations (*Thank you, TSAG*).

The Gaps – Leadership

Missing in 27% of locations

1. Identify and maintain record of safeguards
2. Ensure staff are aware of and adhere to all safeguards
3. Enter into a written agreements with Information Managers
4. Designate a Privacy Officer

The Gaps – Privacy Officer



Missing in 38% of locations.

1. Keep privacy policies and procedures current
2. Ensure that the staff and patients are aware of their obligations
3. Ensure that the vendors are aware of their obligations
4. Monitor compliance with privacy regs
5. Manage privacy breach procedures

The Gaps – Privacy Impact Assessment

“The PIA is not an ‘active’ document.”

A PIA demonstrates that an organization has:

1. Considered all current privacy risks to health information in the care of the organization
2. Implemented reasonable steps to protect against those risks

PIAs were not readily available or largely out of date.

- Unreferenced policies and procedures
- Recent implementations not assessed
- Policies and procedures designed for clinic structure that is no longer valid

BRIGHTSQUID

The Gaps – Paper Records

“Paper patient records are common.”

1. Paper records are difficult to track, access audits are nearly impossible
2. Paper records create more work when sharing
3. Backup is time consuming and difficult
4. Business continuity is near impossible (flood, fire)

The Gaps – Unsecure Communications

Use unsecure communications expecting information is kept private.

Those that claimed the use of secure email listed unsecure services.

Communication with Patients	% of Locations Using
Phone	100%
Email	31.8%
Text Message	63.6%
Secure Email	18.2%
Mail	22.7%
Social media	27.3%
Video conferencing	27.3%

Communication with Professionals	% of Locations Using
Fax	95.5%
Phone	100%
Email	50%
Text Message	31.8%
Secure email	54.5%
Mail	36.4%
Video Conferencing	63.6%

The Gaps – Documentation

Document	Compliant Locations
Password Requirements	62%
Mobile Device/Wireless Use Policy	42%
Privacy Breach Response Plan	50%
Data Retention Policy	33%
Security Policy	46%
Privacy Training Log	46%

The Gaps – Policy Reviews

Policy	Reviewed Annually
Access controls	35.71%
Software policy	42.86%
Mobile computing policy	42.86%
Network firewall policy	42.86%
Wireless configuration	28.57%
Hardware inventory	50.00%

The Gaps – Agreements

Information Manager Agreements – Delegation of responsibility

Vendor	% With Vendor	% With Agreements*
Third-party Backup	**45%**	**30%**
Secure Email Provider	**59%**	**15%**
Third-party Shredding	**41%**	**0%**
Security Services	59%	0%
Cleaning Services	54.5%	0%
Appointment Reminder Software	**45.5%**	**0%**
AVERAGE	**52.6%**	**9%**

* “Unknown” counted as none.

BRIGHTSQUID

Recommendations

Recommendations

1. Deploy a custom privacy training curriculum. Implement a training log.
2. Fill gaps in policies and procedures and enable technology adoption.
3. Implement controls for paper records including access logs and retention guidelines.
4. Ensure up-to-date Privacy Impact Assessments

BRIGHTSQUID

Recommendations

5. Move off paper to a single EMR at each location
6. Implement backup procedure for all patient records
7. Implement secure and compliant communication services
8. Conduct software review and hardware audit at least annually

BRIGHTSQUID

Understand Real Privacy Risk

Breaches In Real Life

1. **Human error a factor in 88% of breaches**
2. Mistakes and mis delivery:
   - Cc email lists instead of Bcc
   - Misdialed fax
3. Ransomware:
   - 4 of 10 top attacks in 2023 hit healthcare
   - Encrypt and exfiltrate data
4. Impact quality of care and access

BRIGHTSQUID

Breach Causes in Alberta

Cause	Frequency
1. Cyber Attack	24
2. Ransomware	22
3. Mistake	19
4. Compromised Credentials	12
5. Theft	9
6. Phishing	8
7. “Lost in the Mail”	3
8. Credential Stuffing	2

IT overlap across most categories (*1+2+4+6+8*).

Email makes room for Mistakes:

- 4 were forgetting to Bcc in email
- 4 were misdirected emails

SOURCE: All Breach Notification Decisions published by the OIPC in 2022 & 2023:

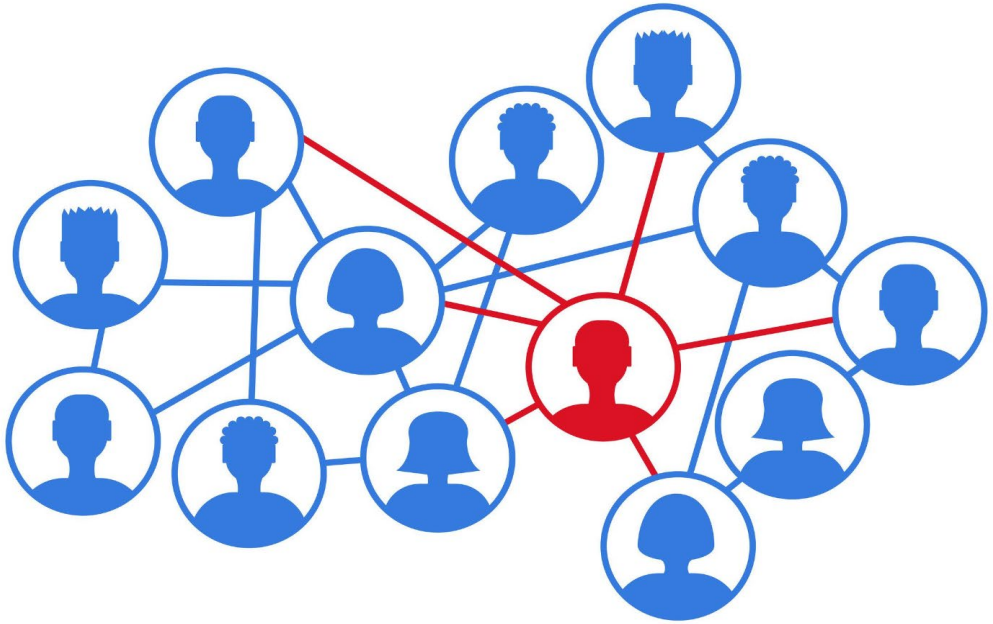
https://oipc.ab.ca/decisions/breach-notification-decisions/

BRIGHTSQUID

Why Mistakes Happen:

Daily work pressures can override training in favour of speed and convenience.

- Urgency
- High frequency tasks
- Demanding workloads
- Too much process
- Stress



BRIGHTSQUID

#1 Breach Prevention = Reduce Overwhelm

1. Plan – Implement policies and review schedules
2. Ensure training – Knowledge eliminates stress
3. Eliminate excess manual effort/process:
   - Printing/scanning
   - Envelope stuffing
   - Placing dead-end phone calls
   - Manual form data entry
   - Replace typing with templates
   - Complex IT configurations

BRIGHTSQUID

Vulnerabilities:

1. Untrained staff
2. Outdated Systems & Software
3. Third-Parties
4. Email:
   - Ransomware
   - Phishing
   - Mistakes

Address with:

1. Training curriculum & logs
2. Software audits
3. Partner agreements with responsibilities
4. Brightsquid Secure-Mail:
   - Ransomware blocking
   - Closed system
   - Automatic breach prevention

BRIGHTSQUID

Safe and Appropriate Communication

Indigenous Patient Connectivity Considerations

Working with the Alberta Indigenous Virtual Care Clinic we have learned:

- Some patients have a variable home address
- Phone numbers can subject to frequent change
- Cellular coverage may be weak in rural areas
- Not everyone lives in a connected home
- **Email or social media can *seem* the best way**

BRIGHTSQUID

Stronger Patient Connection & Support

Provide Choice & Flexibility:

- Phone
- In-person
- Secure messaging
- Virtual visits
- Website-based intake
- Allow extra time in appointments
  - *How can you support clinic capacity?*
- Support more than one concern

Stronger Patient Connection & Support

AIVCC use of Secure Messaging for Patient Support:

Remote screening & assessment:

- Mental health
- Diabetes, Vaccines
- Chronic condition self-management support

Secure appointment reminders:

- Include instructions
- Collect form data online in advance
- Improve access to care

Asynchronous appointment requests:

- After hours delivery
- Patients send supportive documents (pictures)

Collaboration:

- Shared team inbox for constant coverage
- Usable with providers and patients for continuity through transfers of care

BRIGHTSQUID

Email Privacy Risks

- 85% of Ransomware+ enters through email inbox.
- Untraceable path across unsecure Internet. Hackers watch for health data.
- Was info subject to rules from other jurisdictions?
- Webmail services read personal inboxes.

BRIGHTSQUID

Text Messaging Privacy Risks

- The phone network can be hacked easily.
- Messages stored on phone company servers with no way to delete them.
- Service providers do not treat SMS data as health information.
- No way to pull back info sent to the wrong number.

Acceptable use: **“Please contact the clinic.”**

BRIGHTSQUID

Social Media Privacy Risks

- Platforms analyze messages for marketing and sell to third parties.
- Accounts and devices often shared.
- No automatic logout.
- Where is information stored, subject to which rules?

Acceptable use: **“Please contact the clinic.”**

BRIGHTSQUID

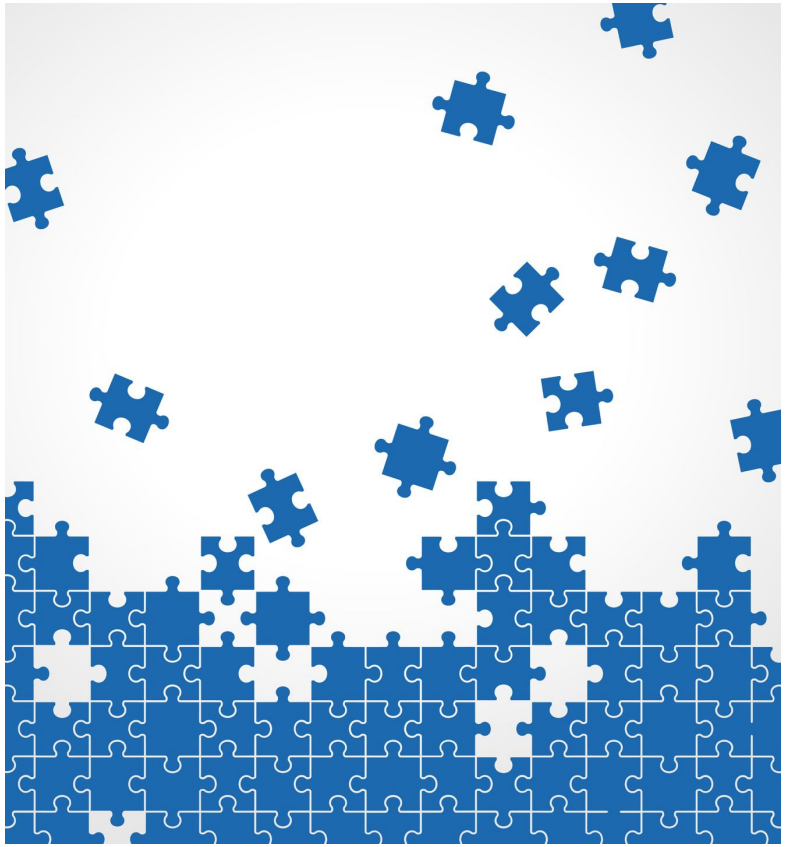
Secure Communication Safeguards

- Ensure security and compliance:
  - Closed system, not the open Internet
  - No data snooping/marketing use
  - Encryption in transit and at rest
- Technical safeguards:
  - Ransomware blocking
  - Always on encryption
  - Forced Bcc vs Cc (for patient groups)
  - Multi-point identity validation
  - Protocol for reliable recall
- Ensure strong passwords & no sharing

Solving Communication Challenges

Hire services that:

- ❑ Use an identifier unique to recipients over the long term
- ❑ Have a familiar user-friendly interface
- ❑ Have low bandwidth demands
- ❑ Can be safely accessed over any connection
- ❑ Streamline administrative processes
- ❑ Don’t require ongoing IT configuration
- ❑ Support individual user accounts
- ❑ Provide true two-way communication
- ❑ Provide patient user support



BRIGHTSQUID

What's Next?

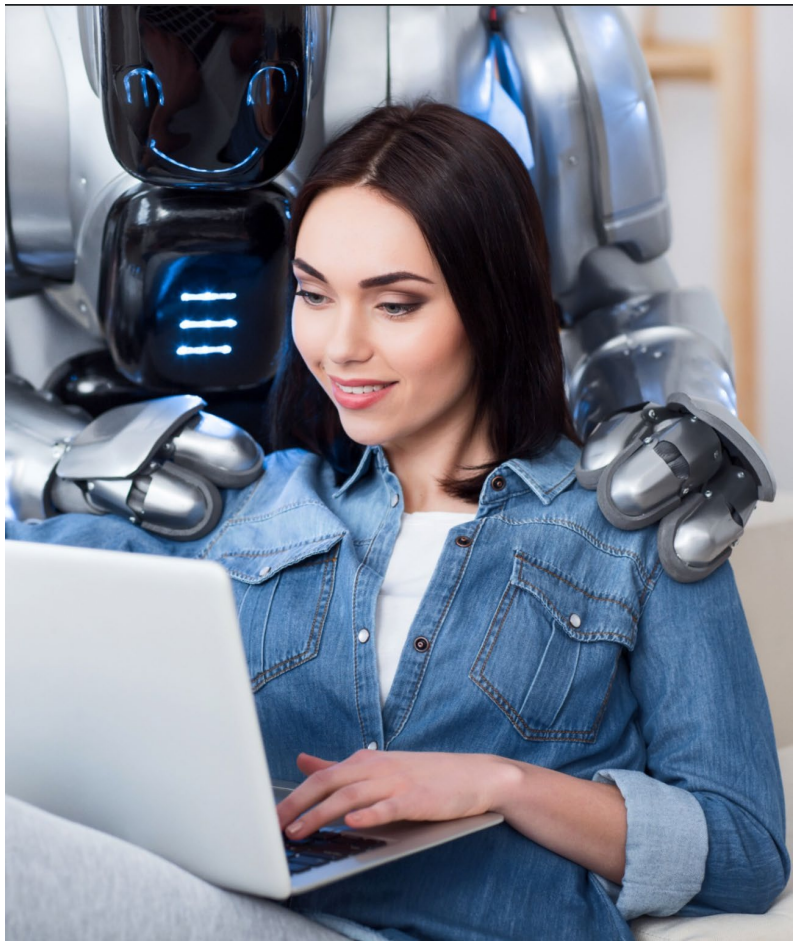
Artificial Intelligence in Healthcare

AI used in healthcare today:

- **Diagnostic Assistance** - diagnostic imaging is analyzed by AI to automate disease detection
- **Treatment Planning** - personalized automated treatment planning
- **Transcription -** Taking encounter notes from the appointment

More questions than answers:

- What data is being collected, used, disclosed?
- Where/how is the data being analyzed?
- What level of anonymity is used?
- What is the purpose of collection, use, disclosure?
- Will vendor enter into necessary agreements/provide documentation?



BRIGHTSQUID

Regulatory Developments & Expectations

Federal:

- Privacy Program requirements and disclosure
- AI rules – “Right to object/restrict processing”
- Bill C-72, the Connected Care for Canadians Act
- Organizations fined for falling victim to ransomware & phishing
- “Protecting Employee Privacy in the Modern Workplace” Resolution by Canadian Privacy Commissioners

Regulatory Developments & Expectations

Provincial:

- AB changes and new interpretations will require revisions to agreements at minimum
- AB MAPS Indigenous Primary Health Care Advisory Panel:
  - Culturally safe and appropriate care
  - Address inequities in Access, Integration, Quality
  - Indigenous peoples as partners.
- BC Anti-Racism Data Act:
  - Improving programs and services so more people feel safe getting the help they need.
  - Increase transparency & accountability, prevent and reduce harms to Indigenous Peoples and racialized communities.
- ON privacy commissioner can now impose fines
- More “PIA type” requirements

jeff.mackay@brightsquid.com

BRIGHTSQUID

THANQ

brightsquid.com

BRIGHTSQUID