



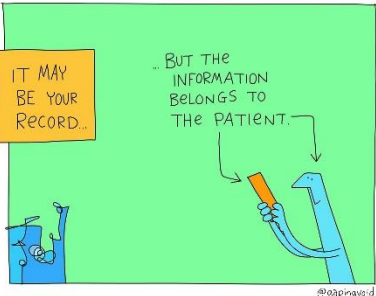

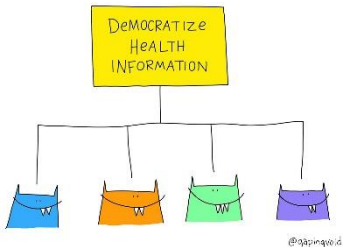

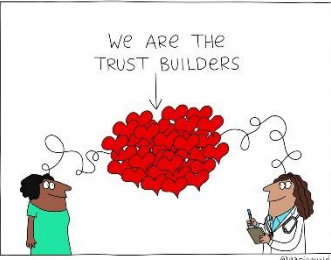


Summary of Privacy Training

<p>1.</p>		<p>If you don't know what to do or have a privacy question – ask for advice from the Privacy Officer, your supervisor, your regulatory College or professional association.</p> <p>Ask others their “go to phrases” for dealing with privacy issues. Talk about ways in which you can support each other to be more privacy respectful.</p>
<p>2.</p>		<p>If there is a significant risk of serious bodily harm to a patient or someone else and sharing information would reduce or eliminate that risk – share the information. Usually that will mean calling 9-1-1 or police or their family or another person to meet your duty to warn. Only share the minimal health information necessary to warn. If unsure what to do – seek advice. In an emergency if you cannot get timely advice err on the side of protecting safety.</p>
<p>3.</p>		<p>Do not look at health records if you don't have a legitimate job reason to do so. Think: “am I allowed and supposed to look at this?” Do not look at health records out of your interest or curiosity. Do not look at your family or friend’s health record or your own health record without following the procedures any other patient or substitute decision-maker or third party would have to follow to get a copy. Electronic systems are audited.</p>
<p>4.</p>		<p>Report all privacy complaints, incidents and breaches to your Privacy Officer.</p>
<p>5.</p>		<p>You must be authorized before you take any patient information off site (in paper or on a laptop or USB key or mobile device). If you have not been told you are allowed to take patient information off-site – don't! Laptops, USB keys and other mobile devices must be encrypted if transporting patient information. Do not save patient information on the hard drive if the device is unencrypted. Do not store patient information at home. Using the secure remote access is fine. If you have questions, please ask the Privacy Officer.</p>

<p>6.</p>		<p>This is not a trick. Anticipate when you will need to communicate and clarify how they want to hear from you. Do they want you to leave detailed messages on voicemail? Do they want you to share information with their spouse/partner/parents/children/roommate if they call to make an appointment or get test results? Is there any sensitive information they do not want shared? Clinicians need to make it obvious to front line staff what can and cannot be shared by phone or in person or online and with whom. When in doubt – do not share information with family members or on voice messages.</p>
<p>7.</p>		<p>“Circle of care” means clinical staff can share patient information with other health care providers to coordinate health care to shared patients relying on implied consent. Hospitals, pharmacies, laboratories, primary care teams, long term care homes, community care providers, regulated health professionals and other health agencies and individuals providing direct health care to a shared patient can be IN the circle of care. The following ARE NOT in the circle of care: police, insurance companies, employers, family members, landlords, WSIB or CAS. If the patient says “don’t share information with the hospital or another health care provider” the circle of care ends. In that case – you would need express consent to share information going forward.</p>
<p>8.</p>		<p>You need express consent to share patient information with anyone who is not a health care provider (like insurance companies, employers, family members (who are not substitute decision- makers), lawyers) unless you are otherwise permitted or required by law to disclose. Express consent can be verbal or written (but you should chart all verbal discussions in the patient’s record).</p> <p>When a third party such as CAS, WSIB, or an insurance company or lawyer or regulatory College says "you are required by law to share with me" ask them to put their request in writing and include the section of the law to which they are referring. Include that written instruction in the patient’s record. If you are unsure whether they have given you sufficient documentation to require you to disclose, consult with the Privacy Officer.</p>

<p>9.</p>		<ul style="list-style-type: none"> • Person of any age who is capable can make decisions about release of everything in their own health record • Person of any age who is incapable needs a substitute decision-maker to release anything in health record • Person who is under the age of 16 and capable can make decisions about release of everything in their own health record AND a parent can also consent to release of information about any treatment or counseling that child did not consent to on their own BUT NOT IF THE CAPABLE CHILD OBJECTS TO PARENT MAKING SUCH DECISIONS <p>To be “capable” a patient must be (1) able to understand the information that is relevant to making a privacy decision; and (2) able to appreciate the reasonably foreseeable consequences of the decision. Patients who make their own treatment and counseling decisions generally also make decisions about how information about their treatment and counseling is collected, used and disclosed. Similarly, if a patient is incapable of making treatment decisions the substitute decision-maker usually makes privacy decisions for the patient.</p>
<p>10.</p>		<p>Patients have a right to access their records of personal health information. The main source will be the “chart” (or other patient records) – but you may also have personal health information in other formats like emails or reports or transfer notes. You have up to 30 days to respond to access requests – with the potential for an extension. There are some limits to the right of access (such as if to provide access could cause harm). Patients may also ask for their records to be corrected. You must correct records if they are inaccurate or incomplete for the purposes for which you hold the records.</p>
<p>11.</p>		<p>Have hard to guess passwords. Do not leave your password signed in when you leave a computer or a room. Do not share your password with your colleagues or anyone else. Be on the lookout for malicious emails. Do not open emails or click on links if you are unsure of the sender. Do not pick up and use unidentified USB keys. Do not let strangers into your server room or telecom room.</p>

<p>12.</p>	 <p>A yellow box at the top contains the text "DEMOCRATIZE HEALTH INFORMATION". Below it, four lines connect to four smaller boxes, each containing a white letter 'W'. The boxes are colored blue, orange, green, and purple from left to right. A small signature "@gapingvoid" is at the bottom right.</p>	<p>Information is power. Design your health information systems so that patients can participate and co-create. Help patients understand their privacy rights.</p>
<p>13.</p>	 <p>A blue box at the top left says "PROTECT PAPER". A line connects it to a purple box on the right that says "keep ALL PAPER RECORDS OUT OF SIGHT OF VISITORS". Below the blue box, a sign on a wooden post says "SHRED IT ALL!". A small signature "@gapingvoid" is at the bottom right.</p>	<p>Do not recycle or throw out personal health information. Shred it! Be careful to keep paper records out of sight of visitors. If providing a copy of a record to a patient, mark it "Patient Copy".</p>
<p>14.</p>	 <p>Text at the top says "WE ARE THE TRUST BUILDERS" with an arrow pointing down to a large, dense pile of red hearts. Two cartoon characters, a woman on the left and a man on the right, are looking at the hearts. A small signature "@gapingvoid" is at the bottom right.</p>	<p>Building trust is essential to our work. Being privacy respectful is one of the key ways we can demonstrate we care about the patients we serve.</p>